Docket No.: 31869-201591
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Matsumura et al.

Application No.: Not Yet Assigned

Confirmation No.: N/A

Filed: Concurrently Herewith

Art Unit: N/A

For: METHOD OF RECONSTRUCTING A SECRET, SHARED SECRET RECONSTRUCTION APPARATUS, AND SECRET RECONSTRUCTION SYSTEM

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

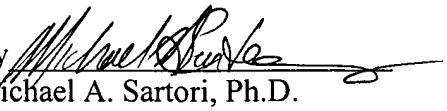
Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Japan	2003-067834	March 13, 2003

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: March 12, 2004

Respectfully submitted,

By 

Michael A. Sartori, Ph.D.
Registration No.: 41,289
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)
Attorney/Agent For Applicant

MAS/trl
DC2-530685

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月１３日

出願番号
Application Number: 特願２００３－０６７８３４

[ST. 10/C]: ［ＪＰ２００３－０６７８３４］

出願人
Applicant(s): 沖電気工業株式会社

２００３年１１月２１日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０９６７４１

【書類名】　特許願
【整理番号】　MA001423
【提出日】　平成15年 3月13日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/08
【発明者】
【住所又は居所】　東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
【氏名】　松村　靖子
【発明者】
【住所又は居所】　東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
【氏名】　中川　聰
【発明者】
【住所又は居所】　東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
【氏名】　圓藤　康平
【特許出願人】
【識別番号】　000000295
【氏名又は名称】　沖電気工業株式会社
【代理人】
【識別番号】　100083840
【弁理士】
【氏名又は名称】　前田　実
【選任した代理人】
【識別番号】　100116964
【弁理士】
【氏名又は名称】　山形　洋一

【手数料の表示】

【予納台帳番号】　007205

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003703

【包括委任状番号】　0101807

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　秘密再構成方法、分散秘密再構成装置、及び秘密再構成システム

【特許請求の範囲】

【請求項１】　秘密分散法を用いて、もとの秘密情報からｎ個の第１の分散情報を生成し、上記ｎ個の第１の分散情報をｎ人（２≦ｎ）のメンバのそれぞれに配布している場合に、上記ｎ人のメンバのうちのｔ（２≦ｔ≦ｎ）人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法において、

上記集まったｔ人のメンバのそれぞれが、秘密分散法を用いて、自分自身が保持する第１の分散情報からｔ個の第２の分散情報を生成し、上記集まったｔ人のメンバのそれぞれに配布する工程と、

上記集まったｔ人のメンバのそれぞれが、自分自身が生成した第２の分散情報及び他のメンバから自分自身が受け取った（ｔ－１）個の第２の分散情報を用いた分散計算により、上記もとの秘密情報を再構成するためのｔ個の中間計算結果を生成する工程と、

上記ｔ個の中間計算結果から、上記もとの秘密情報を再構成する工程と

を有することを特徴とする秘密再構成方法。

【請求項２】　上記第１の分散情報は、上記ｎ個の第１の分散情報をすべて加算した値が、上記もとの秘密情報となるような秘密分散法により得られたことを特徴とする請求項１に記載の秘密再構成方法。

【請求項３】　上記第２の分散情報は、分散情報をすべて加算した値が第１の分散情報となるような秘密分散法により得られたことを特徴とする請求項１又は２のいずれかに記載の秘密再構成方法。

【請求項４】　あるメンバが生成した上記中間計算結果は、上記あるメンバ自身が生成した第２の分散情報及び上記あるメンバ自身が受け取った（ｔ－１）個の第２の分散情報をすべて加算することによって得られたことを特徴とする請求項１から３までのいずれかに記載の秘密再構成方法。

【請求項５】　上記ｎ個の第１の分散情報は、上記メンバのそれぞれを識別するためのメンバＩＤを用いたしきい値秘密分散法により得られたことを特徴と

する請求項１に記載の秘密再構成方法。

【請求項６】　上記第２の分散情報は、上記集まったｔ人のメンバのそれぞれが持つ第１の分散情報を、メンバＩＤを用いたしきい値秘密分散法、又は、分散情報をすべて加算することにより秘密再構成を行うことができる秘密分散法を用いて秘密分散することにより得られたことを特徴とする請求項１又は５のいずれかに記載の秘密再構成方法。

【請求項７】　あるメンバが生成した上記中間計算結果は、上記あるメンバ自身が生成した第２の分散情報及び上記あるメンバ自身が受け取った（ｔ－１）個の第２の分散情報を、上記あるメンバのメンバＩＤに基づく係数を用いて線形結合計算することによって得られたことを特徴とする請求項１、５、６のいずれかに記載の秘密再構成方法。

【請求項８】　上記集まったｔ人のメンバに対して、互いに重複しない仮メンバＩＤを生成して配布する工程をさらに有し、

上記もとの秘密情報を再構成するための上記中間計算結果を、上記仮メンバＩＤを用いた分散計算により算出し、上記中間計算結果及び上記仮メンバＩＤから、上記もとの秘密情報を再構成する

ことを特徴とする請求項１、２、４、５、７のいずれかに記載の秘密再構成方法。

【請求項９】　秘密分散法により上記集まったｔ人のメンバのメンバＩＤから第３の分散情報を生成し、上記集まったｔ人のメンバに配布する工程をさらに有することを特徴とする請求項１、３、５、６、８のいずれかに記載の秘密再構成方法。

【請求項１０】　秘密分散法を用いて、もとの秘密情報からｎ個の第１の分散情報を生成し、上記ｎ個の第１の分散情報をｎ人（２≦ｎ）のメンバのそれぞれに配布している場合に、上記ｎ人のメンバのうちのｔ（２≦ｔ≦ｎ）人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法において分散計算を行う複数の分散秘密再構成装置の内の１台であって、上記各メンバが管理する分散秘密再構成装置において、

この分散秘密再構成装置が保有する第１の分散情報を秘密分散法を用いて分散

し、第２の分散情報として他の分散秘密再構成装置に配布する秘密分散手段と、

上記秘密分散手段からの出力と、上記他の分散秘密再構成装置から受け取った第２の分散情報を用いて、上記もとの秘密情報を再構成するための中間計算結果を、分散計算により算出する分散秘密再構成計算手段と、

上記分散秘密再構成計算手段の出力である上記中間計算結果を送信する送信手段と

を有することを特徴とする分散秘密再構成装置。

【請求項１１】　秘密分散法を用いて、もとの秘密情報からｎ個の第１の分散情報を生成し、上記ｎ個の第１の分散情報をｎ人（２≦ｎ）のメンバのそれぞれに配布している場合に、上記ｎ人のメンバのうちのｔ（２≦ｔ≦ｎ）人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法において分散計算を行う複数の分散秘密再構成装置の内の１台であって、上記各メンバが管理する分散秘密再構成装置において、

この分散秘密再構成装置が保有する第１の分散情報を秘密分散法を用いて分散し、第２の分散情報として他の分散秘密再構成装置に配布する秘密分散手段と、

上記秘密分散手段からの出力と、上記他の分散秘密再構成装置から受け取った第２の分散情報を用いて、上記もとの秘密情報を再構成するための中間計算結果を、分散計算により算出する分散秘密再構成計算手段と、

上記分散秘密再構成計算手段からの出力と、上記他の分散秘密再構成装置の出力を受け取り、それらの出力から、上記もと秘密情報を再構成する秘密再構成手段と

を有することを特徴とする分散秘密再構成装置。

【請求項１２】　上記分散秘密再構成計算手段からの出力と、他の分散秘密再構成装置のからの出力を受け取り、それらの出力から、もと秘密情報を再構成する秘密再構成手段をさらに有することを特徴とする請求項１０に記載の分散秘密再構成装置。

【請求項１３】　上記秘密分散手段は、分散情報をすべて加算した値がもとの秘密情報となるような秘密分散法を用いることを特徴とする請求項１０から１２までのいずれかに記載の分散秘密再構成装置。

【請求項１４】　上記分散秘密再構成計算手段は、上記秘密分散手段からの出力と、他の分散再構成装置から受け取った第２の分散情報をすべて加算する加算手段を含むことを特徴とする請求項１０から１３までのいずれかに記載の分散秘密再構成装置。

【請求項１５】　上記秘密分散手段は、メンバＩＤを用いたしきい値秘密分散法を用いることを特徴とする請求項１０、１１、１２、１４のいずれかに記載の分散秘密再構成装置。

【請求項１６】　上記分散秘密再構成計算手段は、上記秘密分散手段からの出力と、秘密通信路を通して他の分散秘密再構成装置から受け取った第２の分散情報を、メンバＩＤから計算される係数を用いて線形結合計算をする線形結合計算手段を含むことを特徴とする請求項１０、１１、１２、１３、１５のいずれかに記載の分散秘密再構成装置。

【請求項１７】　上記秘密分散手段は、この分散秘密再構成装置に配布された仮メンバＩＤを用いたしきい値秘密分散法を用いることを特徴とする請求項１０、１１、１２、１４、１６のいずれかに記載の分散秘密再構成装置。

【請求項１８】　上記秘密分散手段は、この分散秘密再構成装置が保有するメンバＩＤを秘密分散法を用いて分散し、第３の分散情報として他の分散秘密再構成装置に配布し、

上記分散秘密再構成計算手段は、上記秘密分散手段から出力される第２及び第３の分散情報と、他の分散秘密再構成装置から受け取った第２及び第３の分散情報を用いて、秘密再構成の中間計算結果を、分散計算により算出する

ことを特徴とする請求項１０、１１、１２、１３、１７のいずれかに記載の分散秘密再構成装置。

【請求項１９】　上記分散秘密再構成計算手段は、

上記秘密分散手段から出力される第２及び第３の分散情報と、他の分散秘密再構成装置から受け取ったの第２及び第３の分散情報を用いて、第２の分散情報に対する、第３の分散情報から計算される係数を分散計算した結果と、その各第２の分散情報との分散乗算を行う項計算手段と、

上記項計算手段の出力を、すべて足し合わせる加算手段と

を含むことを特徴とする請求項１０、１１、１２、1"3、1"7，１８のいずれかに記載の分散秘密再構成装置。

【請求項２０】　上記項計算手段は、

異なる第３の分散情報同士の差分をとる差分計算手段と、

上記差分計算手段の出力を分散乗算する第１の多項分散乗算手段と、

上記第１の多項分散乗算手段の出力の逆元を分散計算する分散逆元計算手段と、

第３の分散情報を分散乗算する第２の多項分散乗算手段と、

上記分散逆元計算手段の出力と、第２の多項分散乗算手段の出力と、対応する第２の分散情報とを分散乗算する第３の多項分散乗算手段と、

を含むことを特徴とする請求項１０、１１、１２、１３、１７、１８、１９のいずれかに記載の分散秘密再構成装置。

【請求項２１】　上記第１、第２、及び第３の多項分散乗算手段はそれぞれ、分散乗算する値の個数よりも１小さい個数の、２つの値を分散乗算する二項分散乗算手段を含むことを特徴とする請求項１０、１１、１２、１３、１７、１８、１９、２０のいずれかに記載の分散秘密再構成装置。

【請求項２２】　上記二項分散乗算手段はそれぞれ、

入力される２つの入力を掛け合わせる乗算手段と、

上記乗算手段の出力を、仮メンバＩＤを用いたしきい値秘密分散法で分散し、第４の分散情報として他の分散秘密再構成装置に対して秘密通信路を通して配布する第２の秘密分散手段と、

上記第２の秘密分散手段からの出力と、他の分散秘密再構成装置から秘密通信路を通して受け取った第４の分散情報を、仮メンバＩＤから計算される係数を用いて線形結合計算をする線形結合計算手段と、

を含むことを特徴とする請求項１０、１１、１２、１７、１８、１９、２０、２１のいずれかに記載の分散秘密再構成装置。

【請求項２３】　上記二項分散乗算手段はそれぞれ、

入力される２つの入力を掛け合わせ、さらに仮メンバＩＤから計算される係数を掛け合わせる第１の乗算手段と、

入力される第１の入力と、他の分散秘密再構成装置の対応するに項分散乗算手段への第２の入力との乗算結果を、秘密通信路を通して紛失通信を行うことにより計算する第１の通信計算手段と、

入力される第２の入力と、他の分散秘密再構成装置の対応するに項分散乗算手段への第１の入力との乗算結果を、秘密通信路を通して紛失通信を行うことにより計算する第２の通信計算手段と、

第１の通信計算手段の出力と第２の計算手段の出力を足し合わせる加算手段と、

上記加算手段の出力に、仮メンバＩＤから計算される係数を掛け合わせる第２の乗算手段と、

上記第１の乗算手段の結果と上記第２の乗算手段の結果とをすべて足し合わせる第２の加算手段と、

を含むことを特徴とする請求項１０、１１、１２、１７、１８、１９、２０、２１のいずれかに記載の分散秘密再構成装置。

【請求項２４】　上記二項分散乗算手段はそれぞれ、

入力される２つの入力を掛け合わせる第１の乗算手段と、

入力される第１の入力と、他の分散秘密再構成装置の対応する二項分散乗算手段への第２の入力との乗算結果を、秘密通信路を通して紛失通信を行うことにより計算する第１の通信計算手段と、

入力される第２の入力と、他の分散秘密再構成装置の対応する二項分散乗算手段への第１の入力との乗算結果を、秘密通信路を通して紛失通信を行うことにより計算する第２の通信計算手段と、

第１の通信計算手段の出力と第２の計算手段の出力を足し合わせる加算手段と、

上記第１の乗算手段の結果と上記加算手段の結果とをすべて足し合わせる第２の加算手段と、

を含むことを特徴とする請求項１０、１１、１２、１３、１８、１９、２０、２１のいずれかに記載の分散秘密再構成装置。

【請求項２５】　上記分散逆元計算手段は、

演算に用いる有限体の大きさから計算される第１の個数の、上記請求項２２、２３又は２４のいずれかに記載の二項分散乗算手段と同じ構成を持つ二項分散乗算手段と、

分散乗算する値の個数が、演算に用いる有限体の大きさから計算される第２の個数である上記請求項２１に記載の第１、第２、及び第３の多項分散乗算手段と同じ構成を持つ多項分散乗算手段と

を含むことを特徴とする請求項１０、１１、１２、１３、１７、１８、１９、２０、２１、２２、２３、２４のいずれかに記載の分散秘密再構成装置。

【請求項２６】　上記分散逆元計算手段は、

乱数を生成する乱数生成手段と、

入力される値とその乱数生成手段の出力とを入力とする、上記請求項２２又は請求項２３のいずれかに記載の二項分散乗算手段と同じ構成を持つ第２の二項分散乗算手段と、

上記第２の二項分散乗算手段からの出力と、秘密通信路を通して受け取ったほかの分散秘密再構成装置の対応する第２の二項分散乗算手段の出力を、仮メンバＩＤから計算される係数を用いて線形結合計算をする線形結合計算手段と、

上記線形結合計算手段の出力の有限体上の演算における逆元を計算する逆元計算手段と、

上記逆元計算手段の結果を分散し、第５の分散情報として他の分散秘密再構成装置に対して秘密通信路を通して配布する秘密分散手段と、

上記秘密分散手段における第５の分散情報と、その乱数生成手段からの出力と入力とする、上記請求項２２又は請求項２３のいずれかに記載の二項分散乗算手段と同じ構成を持つ第３の二項分散乗算手段と、

を含むことを特徴とする請求項１０、１１、１２、１７、１８、１９、２０、２１、２２、２３のいずれかに記載の分散秘密再構成装置。

【請求項２７】　上記分散逆元計算手段は、

乱数を生成する乱数生成手段と、

入力される値とその乱数生成手段の出力とを入力とする、上記請求項２４に記載の二項分散乗算手段と同じ構成を持つ第２の二項分散乗算手段と、

上記第２の二項分散乗算手段からの出力と、秘密通信路を通して受け取ったほかの分散秘密再構成装置の対応する第２の二項分散乗算手段の出力をすべて足し合わせる加算手段と、

上記線形結合計算手段の出力の有限体上の演算における逆元を計算する逆元計算手段と、

上記逆元計算手段の結果を分散し、第５の分散情報として他の分散秘密再構成装置に対して秘密通信路を通して配布する秘密分散手段と、

上記秘密分散手段における第５の分散情報と、その乱数生成手段からの出力とを入力とする、上記請求項２４に記載の二項分散乗算手段と同じ構成を持つ第３の二項分散乗算手段と、

を含むことを特徴とする請求項１０、１１、１２、１３、１８、１９、２０、２１、２４のいずれかに記載の分散秘密再構成装置。

【請求項２８】　上記分散逆元計算手段は、

乱数を生成する乱数生成手段と、

入力される値とその乱数生成手段の出力とを入力とする、上記請求項２２、２３又は２４のいずれかに記載の二項分散乗算手段と同じ構成を持つ第４の二項分散乗算手段と、

上記第４の二項分散乗算手段の計算結果を、上記請求項２６又は２７に記載の分散秘密再構成装置と同じ構成を持つ分散秘密再構成装置へ送信する送信手段と、

上記請求項２６又は２７に記載の分散秘密再構成装置と同じ構成を持つ分散秘密再構成装置から、上記第５の分散情報を受信する受信手段と、

上記受信した第５の分散情報と、その乱数生成手段からの出力とを入力とする、上記請求項２２、２３又は２４のいずれかに記載の二項分散乗算手段と同じ構成を持つ第５の二項分散乗算手段と

を含むことを特徴とする、請求項１０、１１、１２、１３、１７、１８、１９、２０、２１、２２、２３、２４のいずれかに記載の分散秘密再構成装置。

【請求項２９】　秘密分散法を用いて、もとの秘密情報からｎ個の第１の分散情報を生成し、上記ｎ個の第１の分散情報をｎ人（２≦ｎ）のメンバのそれぞ

れに配布している場合に、上記ｎ人のメンバのうちｔ（"2≦t"≦ｎ）人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

上記請求項１０、１１、１２のいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置と、

上記分散秘密再構成装置の出力から、上記もとの秘密情報を再構成する秘密再構成装置と

を有することを特徴とする秘密再構成システム。

【請求項３０】　秘密分散法を用いて、もとの秘密情報からｎ個の第１の分散情報を生成し、上記ｎ個の第１の分散情報をｎ人（２≦ｎ）のメンバのそれぞれに配布している場合に、上記ｎ人のメンバのうちｔ（２≦ｔ≦ｎ）人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

上記請求項１０から２８までのいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置を有し、

上記複数台の分散秘密再構成装置の内の少なくとも１台以上は、上記分散秘密再構成手段からの出力と、他の分散秘密再構成装置の出力を受け取り、それらの出力から、上記もとの秘密情報を再構成する秘密再構成手段を有する

ことを特徴とする秘密再構成システム。

【請求項３１】　秘密分散法を用いて、もとの秘密情報からｎ個の第１の分散情報を生成し、上記ｎ個の第１の分散情報をｎ人（２≦ｎ）のメンバのそれぞれに配布している場合に、上記ｎ人のメンバのうちｔ（２≦ｔ≦ｎ）人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

上記請求項１０、１１、１２、１３、１４、１６、１８、１９、２０、２１、２４、２５、２７、２８のいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置と、

分散情報をすべて加算した値がもとの秘密情報となるような秘密分散法の再構成を用いて、上記複数台の分散情報再構成装置の出力から、上記もとの秘密情報

を再構成する秘密再構成装置と

を有することを特徴とする秘密再構成システム。

【請求項３２】　秘密分散法を用いて、もとの秘密情報からｎ個の第１の分散情報を生成し、上記ｎ個の第１の分散情報をｎ人（２≦ｎ）のメンバのそれぞれに配布している場合に、上記ｎ人のメンバのうちｔ（２≦ｔ≦ｎ）人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

上記請求項１０、１１、１２、１４、１５、１６のいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置と、

メンバＩＤを用いたしきい値秘密分散法の再構成方法を用いて、上記複数台の分散秘密再構成装置の出力から、上記もとの秘密情報を再構成する秘密再構成装置と、

を有することを特徴とする秘密再構成システム。

【請求項３３】　秘密分散法を用いて、もとの秘密情報からｎ個の第１の分散情報を生成し、上記ｎ個の第１の分散情報をｎ人（２≦ｎ）のメンバのそれぞれに配布している場合に、上記ｎ人のメンバのうちｔ（２≦ｔ≦ｎ）人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

集まったメンバが管理する分散秘密再構成装置に対して、互いに重複しない仮メンバＩＤを生成し、各分散秘密再構成装置に配布して、各分散秘密再構成装置にすべての仮メンバＩＤを公開する仮メンバＩＤ生成手段と、

上記請求項１０、１１、１２、１４、１６、１７、１８、１９、２０、２１、２２、２３、２５、２６、２８のいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置と、

仮メンバＩＤを用いたしきい値秘密分散法の再構成を用いて、上記複数台の分散秘密再構成装置の出力から、上記もとの秘密情報を再構成する秘密再構成装置と、

を有することを特徴とする秘密再構成システム。

【請求項３４】　上記第１の分散情報は、分散情報をすべて加算した値がも

との情報となるような秘密分散法を用いることを特徴とする請求項２９、３０、３１、３２、３３のいずれかに記載の秘密再構成システム。

【請求項３５】　上記第１の分散情報はメンバＩＤを用いたしきい値秘密分散法を用いることを特徴とする請求項２９、３０、３１、３２、３３のいずれかに記載の秘密再構成システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、秘密分散法により各メンバに分散された分散情報からもとの秘密情報を再構成する秘密再構成方法、この秘密再構成方法を実施する際に使用される分散秘密再構成装置、及びこの分散秘密再構成装置を含む秘密再構成システムに関するものである。

【０００２】

【従来の技術】

情報の秘匿のための暗号化に用いる秘密鍵や認証を行うための秘密などの重要な秘密情報を保管する場合、その秘密情報の紛失や破壊の心配と、その秘密情報の盗難の心配がある。秘密情報を紛失や破壊により失ってしまうことへの対策としては、その秘密情報のコピーを作成し保管することが考えられるが、秘密情報のコピーが増えることにより、その秘密情報の盗難の危険性が増してしまう。この問題を解決する方法として、秘密分散法がある。秘密分散法を実施するシステムにおいては、秘密分散装置（演算装置）が、もとの秘密情報を複数の分散情報に分散（符号化）させ、関係者である各メンバ（演算記憶装置）にそれらの複数の分散情報をそれぞれ配布しておき、もとの秘密情報を得る必要がある場合には、秘密再構成装置（演算装置）が、必要なメンバから分散情報を集め、もとの秘密情報の再構成（復元）を行なう。

【０００３】

秘密分散法の一つに、Ｓｈａｍｉｒ法（シャミア法：Shamir's method）と呼ばれる（ｋ，ｎ）しきい値秘密分散法がある（例えば、非特許文献１参照）。非特許文献１に記述された（ｋ，ｎ）しきい値秘密分散法においては、秘密情報を

ｎ（ｎは２以上の整数）個の分散情報に符号化し、ｋ（'ｋはｎ'以下の整数）個以上の分散情報が集まれば、もとの秘密情報を復元することができるが、ｋ－１個以下の分散情報を集めても、もとの秘密情報を全く知ることができないという性質を、多項式補間を用いることにより実現している。

【０００４】

具体的には、次式（１）に示されるようなｋ－１次多項式ｆ（ｘ）を用いてもとの秘密情報を分散する。

$$f(x)=S+R_1x+R_2x^2+\cdots+R_{k-1}x^{k-1} \quad \cdots(1)$$

ここで、Ｓは、もとの秘密情報であり、R_1，R_2，…，R_{k-1}は、分配者が決める乱数である。

【０００５】

分散情報が配布されるｎ人の各メンバにメンバＩＤとして、m_1，m_2，…，m_nが付与されている場合に、メンバＩＤ＿m_j（ｊ＝１，２，…，ｎ）に対する分散情報Xm_jは、上記式（１）を用いて、次式（２）のように計算できる。

$$Xm_j=f(m_j)=S+R_1m_j+R_2(m_j)^2+\cdots+R_{k-1}(m_j)^{k-1} \quad \cdots(2)$$

【０００６】

図１は、（ｋ，ｎ）しきい値秘密分散法に基づく秘密分散を実施する秘密分散計算部１０１の動作を説明するための図である。図１に示されるように、秘密分散計算部１０１は、もとの秘密情報Ｓ及びこの秘密情報の分散情報が配布されるメンバ全員のメンバＩＤ＿m_j（ｊ＝１，２，…，ｎ）を受け取り、もとの秘密情報Ｓに基づいて上記式（１）の多項式ｆ（ｘ）を生成し、その多項式ｆ（ｘ）及びメンバＩＤ＿m_jに基づいて、各メンバＩＤ＿m_jに対応する分散情報Xm_jを、上記式（２）を用いて生成して出力する。出力した各分散情報Xm_jはそれぞれ、対応するメンバＩＤを持つメンバに秘密裏に配布する。

【０００７】

各メンバに配布した分散情報からもとの秘密情報Ｓを再構成する際には、分散情報が分配されたｎ人のメンバのうちｔ人（$k \leqq t \leqq n$）のメンバを集め、集め

られたｔ人のメンバのメンバＩＤ__m'１，m'２，…，m'ｔと分散情報Ｘm'１，Ｘm'２，…，Ｘm'ｔを持ち寄り、次式（３）及び（４）を用いて、もとの秘密情報Ｓを計算する。

【数１】

$$S = r_{m'_1} X_{m'_1} + r_{m'_2} X_{m'_2} + \cdots + r_{m'_t} X_{m'_t}$$
$$= \sum_{j=1}^{t} r_{m'_j} X_{m'_j} \qquad (3)$$

$$r_{m'_j} = (m'_1 \times m'_2 \times \cdots \times m'_t / m'_j)$$
$$/((m'_1 - m'_j) \times (m'_2 - m'_j) \times \cdots \times (m'_{j-1} - m'_j) \times (m'_{j+1} - m'_j) \times$$
$$\cdots \times (m'_t - m'_j))$$
$$= \prod_{\substack{i=1 \\ i \neq j}}^{t} m'_i / (m'_i - m'_j) \qquad (4)$$

【０００８】

【非特許文献１】

岡本龍明他、「現代暗号」（産業図書）、第２１４－２１６ページ及び第２２７－２３６ページ

【０００９】

【発明が解決しようとする課題】

しかしながら、上記した方法により、もとの秘密情報Ｓの再構成を行う場合には、集まったメンバのメンバＩＤ__m'１，m'２，…，m'ｔや、そのメンバの分散情報Ｘm'１，Ｘm'２，…，Ｘm'ｔを公開しなければ、もとの秘密情報Ｓを計算することができない。また、秘密再構成を行うセンターのようなものがあった場合であっても、集まったメンバのメンバＩＤ__m'１，m'２，…，m'ｔや分散情報Ｘm'１，Ｘm'２，…，Ｘm'ｔをセンターに対して申告しなければ、もとの秘密情報Ｓを計算することができない。すなわち、集まったメンバを匿名にしたまま秘密情報Ｓを計算することはできなかった。

【００１０】

また、秘密再構成を行うセンターのようなものがない場合には、集まったメンバに、自分の持つ分散情報Ｘm'１，Ｘm'２，…，Ｘm'ｔを公開しなければ、

もとの秘密情報Ｓを求めることができない。すなわち、一旦、もとの秘密情報の再構成を行ってしまうと、メンバに配布した分散情報が露呈してしまうので、その露呈した分散情報を再利用することができず、もう一度秘密情報の分散処理を行う必要があった。

【００１１】

そこで、本発明は上記したような従来技術の課題を解決するためになされたものであり、その目的は、各メンバを匿名にしたまま、各メンバの保有する分散情報を公開せずに、もとの秘密情報の再構成を行うことができる秘密再構成方法、この秘密再構成方法を実施する際に使用する分散秘密再構成装置、及びこの分散秘密再構成装置を含む秘密再構成システムを提供することにある。

【００１２】

【課題を解決するための手段】

本発明の秘密再構成方法は、秘密分散法を用いてある秘密情報からｎ個の第１の分散情報を生成し、前記ｎ個の第１の分散情報をｎ人（２≦ｎ）からなるグループの各メンバにそれぞれ配布している場合に、上記ｎ人のメンバのうちのｔ（２≦ｔ≦ｎ）人のメンバが集まって、もとの秘密情報を再構成する方法である。この秘密再構成方法は、集まったｔ人のメンバのそれぞれが、秘密分散法を用いて自身が保持する第１の分散情報からｔ個の第２の分散情報を生成し、集まったｔ人のメンバのそれぞれに配布する工程と、集まったｔ人のメンバのそれぞれが、自身が生成した第２の分散情報及び入力された（ｔ－１）個の第２の分散情報を用いた分散計算により、もとの秘密情報を再構成するためのｔ個の中間計算結果を生成する工程と、集まったｔ人のメンバのそれぞれが生成したｔ個の中間計算結果からもとの秘密情報を再構成する工程とを有する。

【００１３】

【発明の実施の形態】

≪第１の実施形態≫

［第１の実施形態の概要］

本発明の第１の実施形態においては、もとの秘密情報Ｓを再構成する際に、もとの秘密情報Ｓを再構成するために集まったメンバ（演算記憶装置）が保有する

分散情報を用いてマルチパーティ・プロトコルを実行することにより、各メンバが保有する分散情報を公開せずに、もとの秘密情報Ｓの再構成を行う。なお、第１の実施形態に係る秘密再構成方法は、秘密再構成システムにより実施される。第１の実施形態に係る秘密再構成システムは、各メンバ（演算記憶装置）である分散秘密再構成装置（後述する分散秘密再構成計算部３０１）と、メンバのいずれかに又はメンバとは別のセンターに備えられた演算装置（後述する秘密再構成計算部３０２）とを主要な構成としている。

【００１４】

[マルチパーティ・プロトコルの説明]

次に、マルチパーティ・プロトコルの説明をする。マルチパーティ・プロトコルとは、ある関数への入力値を公開せずに、その関数の計算を集まったメンバで協力して行う方式であり、「分散計算」とも呼ばれる（例えば、前述した非特許文献１参照）。マルチパーティ・プロトコルには、大きく分けて２つの方式がある。第１の方式は、計算するために集まったメンバのうち、どの２人のメンバ間にも、その２人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されていることを前提とする方式である。第２方式は、計算するために集まったメンバ間の通信には、前述した秘密通信路による通信方法に加え、紛失通信と呼ばれる通信手法を用いる方式である。前述した非特許文献１には、マルチパーティ・プロトコルの第２方式における、バイナリ計算（ＮＯＴとＡＮＤの計算）の場合の説明が記載されている。また、マルチパーティ・プロトコルの第２方式の詳細は、後述する第４の実施形態において説明する。

【００１５】

ここでは、有限体要素の計算（加算と乗算の計算）を用いるマルチパーティ・プロトコルの第１方式について説明する。マルチパーティ・プロトコルを実行するメンバがｔ人いる場合を想定する。メンバのそれぞれが、メンバＩＤとしてm_j（ｊ＝１，２，…，ｔ）と、そのメンバ固有の秘密情報Xm_j（ｊ＝１，２，…，ｔ）を所有しており、次式（５）に示される関数値Ｙをマルチパーティ・プロトコルで計算する場合を考える。

$$Y = f(Xm_1, Xm_2, \cdots, Xm_t) \quad \cdots (5)$$

ここで、各メンバのメンバＩＤであるm_j及び秘密情報Xm_j（ｊ＝１，２，…，ｔ）は、有限体ＧＦ（ｑ）（ｑは素数又は素数のべき乗）上の値であるものとする。また、上記式（５）の関数ｆにおける演算は、有限体ＧＦ（ｑ）上の演算であるものとし、したがって、得られる関数値Ｙも、有限体ＧＦ（ｑ）上の値となる。

【００１６】

各メンバ固有の秘密情報Xm_j（ｊ＝１，２，…，ｔ）を、他のメンバに公開しないまま、関数値Ｙを計算するために、マルチパーティ・プロトコルでは、まず、各メンバ固有の秘密情報Xm_j（ｊ＝１，２，…，ｔ）を、（ｋ，ｔ）しきい値秘密分散法を用いて秘密分散し、各メンバに配布する。メンバＩＤがm_jであるメンバの秘密情報がXm_jであるとすると、このメンバは、次式（６）のｋ－１（ｋ≦ｔ）次多項式fm_j（ｘ）を作る。

【数２】

$$fm_j(x)=Xm_j+Rm_{j,1}\,x+Rm_{j,2}\,x^2+\cdots+Rm_{j,k-1}\,x^{k-1} \qquad (6)$$

ここで、$Rm_{j,1}$，$Rm_{j,2}$，…，$Rm_{j,k-1}$は、有限体ＧＦ（ｑ）上の値から選ばれたｋ－１個の乱数である。

【００１７】

秘密情報Xm_jを秘密分散法により分散し、メンバＩＤがm_p（ｐ＝１，２，…，ｔ）であるメンバに対して配布される分散情報を$Xm_{j,p}$と表記する場合に、分散情報$Xm_{j,p}$は、上記式（６）を用いて、次式（７）のよう計算できる。

【数３】

$$\begin{aligned} Xm_{j,p} &= fm_j(m_p) \\ &= Xm_j+Rm_{j,1}(m_p)+Rm_{j,2}(m_p)^2+\cdots+Rm_{j,k-1}(m_p)^{k-1} \end{aligned} \qquad (7)$$

なお、分散情報$Xm_{j,p}$は、メンバＩＤがm_p（ｐ＝１，２，…，ｔ）であるメンバ以外には秘密となるよう、秘密通信路を用いて、メンバＩＤがm_p（ｐ＝

１，２，…，ｔ）であるメンバに配布する。

【００１８】

上記式（６）及び（７）における足し算及び掛け算は、有限体ＧＦ（ｑ）上における加算及び乗算であるものとする。したがって、得られる分散情報$Xm_{j,p}$（ｊ＝１，２，…，ｔ；ｐ＝１，２，…，ｔ）は、有限体ＧＦ（ｑ）上の値である。なお、以下の説明においては、断りがない限り、演算は有限体ＧＦ（ｑ）上で行われるものとする。

【００１９】

以上の処理によって、各メンバは、他の各メンバの秘密情報Xm_jの分散情報$Xm_{j,p}$を持っている状態になる。メンバＩＤがm_jであるメンバは、他のメンバから配布された分散情報（及び自分自身の秘密情報の分散情報）$Xm_{1,j}$，$Xm_{2,j}$，…，$Xm_{t,j}$のｔ個の分散情報を持っていることになる。

【００２０】

ここで、マルチパーティ・プロトコルにおける分散加算（足し算計算）を行う。上記式（５）の関数が、例えば、次式（８）に示されるような、ある２つの入力Xm_A及びXm_Bの足し算となっている場合、

$$Y=f(Xm_1, Xm_2, \cdots, Xm_t)=Xm_A+Xm_B \quad \cdots(8)$$

マルチパーティ・プロトコルでは、各メンバは、入力Xm_A及びXm_Bの分散情報同士の足し算を行うことで、計算結果Ｙの分散情報Ym_j（ｊ＝１，２，…，ｔ）を得ることができる。例えば、メンバＩＤがm_jであるメンバは、入力Xm_A及びXm_Bの分散情報として、それぞれ$Xm_{A,j}$及び$Xm_{B,j}$を持っているので、次式（９）のような計算を行い、計算結果Ｙの分散情報Ym_jを得る。

$$Ym_j=Xm_{A,j}+Xm_{B,j} \quad \cdots(9)$$

【００２１】

次に、マルチパーティ・プロトコルにおける分散乗算（掛け算計算）を説明する。上記式（５）の関数が、例えば、次式（１０）のような、ある２つの入力Xm_A及びXm_Bの掛け算となっている場合、

$$Y=f(Xm_1, Xm_2, \cdots, Xm_t)=Xm_A\times Xm_B \quad \cdots(10)$$

マルチパーティ・プロトコルでは、各メンバは、次のようなステップＳ１０１～

Ｓ１０３の処理を行う。ステップＳ１０１においては、入力Xm_A及びXm_Bの分散情報同士の掛け算を行い、ステップＳ１０２においては、その掛け算結果をさらに、他のメンバに秘密分散して配布し、ステップＳ１０３においては、受け取った側でそれらの再構成を行うことで、計算結果Ｙの分散情報Ym_j（ｊ＝１，２，…，ｔ）を得ることができる。ただし、第１方式における、マルチパーティ・プロトコルの分散乗算では、秘密分散のしきい値ｋは、次式（１１）となっている必要がある。

$k \leqq (t+1)/2$　…（１１）

ここで、上記式（１１）の演算は、有限体ＧＦ（ｑ）上の演算ではなく、通常の実数、整数演算である。

【００２２】

具体的に説明すると、例えば、メンバＩＤがm_jであるメンバは、入力Xm_A及びXm_Bの分散情報として、それぞれ$Xm_{A,j}$及び$Xm_{B,j}$を持っているので、まず、次式（１２）のような計算を行い、途中計算結果$Y'm_j$を得る（上記ステップＳ１０１）。

$$Y'm_j = Xm_{A,j} \times Xm_{B,j} \quad \cdots (12)$$

【００２３】

次に、この途中計算結果$Y'm_j$を次式（１３）のような多項式で秘密分散を行う（上記ステップＳ１０２）。

【数４】

$$f'm_j(x) = Y'm_j + R'm_{j,1}\,x + R'm_{j,2}\,x^2 + \cdots + R'm_{j,k-1}\,x^{k-1} \quad (13)$$

ここで、$R'm_{j,1}$，$R'm_{j,2}$，…，$R'm_{j,k-1}$は、乱数として有限体ＧＦ（ｑ）上の値をｋ－１個選ぶことによって得られる。

【００２４】

次に、メンバＩＤがm_p（ｐ＝１，２，…，ｔ）であるメンバに対して配布する自分の途中計算結果$Y'm_j$の分散情報$Y'm_{j,p}$を、上記式（１３）を用いて、次式（１４）のように計算する。

【数５】

$$Y'm_{j,p} = f'm_j(m_p)$$
$$= Y'm_j + R'm_{j,1}(m_p) + R'm_{j,2}(m_p)^2 + \cdots + R'm_{j,k-1}(m_p)^{k-1} \qquad (14)$$

なお、メンバＩＤがm_p（ｐ＝１，２，…，ｔ）であるメンバ以外には秘密となるよう、秘密通信路を用いてメンバＩＤがm_p（ｐ＝１，２，…，ｔ）であるメンバに配布する。上記式（１４）のような計算で分散した結果、メンバＩＤがm_jであるメンバは、$Y'm_{1,j}$，$Y'm_{2,j}$，…，$Y'm_{t,j}$のｔ個の分散情報を受け取る。

【００２５】

メンバＩＤがm_jであるメンバは、これら分散情報$Y'm_{1,j}$，$Y'm_{2,j}$，…，$Y'm_{t,j}$から、掛け算結果の分散情報Ym_jを次式（１５）及び（１６）のように計算する。

【数６】

$$Ym_j = rm_1 Y'm_{1,j} + rm_2 Y'm_{2,j} + \cdots + rm_n Y'm_{n,j}$$
$$= \sum_{i=1}^{t} rm_j Y'm_{i,j} \qquad (15)$$

$$rm_j = (m_1 \times m_2 \times \cdots \times m_t / m_j)$$
$$/((m_1 - m_j) \times (m_2 - m_j) \times \cdots \times (m_{j-1} - m_j) \times (m_{j+1} - m_j) \times \cdots \times (m_t - m_j))$$
$$= \prod_{\substack{i=1 \\ i \neq j}}^{t} m_i / (m_i - m_j) \qquad (16)$$

この計算は、秘密情報の再構成時の計算（前述した式（３））と同様のものである（上記ステップＳ１０３）。

【００２６】

上記のように、マルチパーティ・プロトコルを用いれば、各メンバ同士が秘密通信を行って計算処理をすることにより、入力値を公開せずに、与えられた関数の計算を行うことができる。

【００２７】

［第１の実施形態の構成］

第１の実施形態は、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報Ｓを、（ｋ，ｎ）しきい値秘密分散法ではなく、単純な加減算による秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。すなわち、図２に示されるように、秘密分散法を用いてもとの秘密情報Ｓから分散情報を生成し、生成された分散情報が各メンバに配布されている場合を前提とする。図２は、秘密分散法を実施する秘密分散計算部２０１の動作を説明するための図である。秘密分散計算部２０１は、前述した図１の秘密分散計算部１０１とは動作が異なり、次のような計算を行う。ここで、秘密分散計算部２０１へ入力されるもとの秘密情報をＳ（これは、有限体ＧＦ（ｑ）上の要素とする）とし、分散情報が配布されるメンバがｎ人であるとする。秘密分散計算部２０１は、まず、有限体ＧＦ（ｑ）から乱数をｎ－１個選ぶ。それらの乱数X_1，X_2，…，X_{n-1}から、次式（１７）を満たすX_nを求める。

$$X_n = S - (X_1 + X_2 + \cdots + X_{n-1}) \quad \cdots (17)$$

【００２８】

秘密分散計算部２０１は、上記式（１７）により得られた値X_1，X_2，…，X_nを出力し、各メンバに重複しないように配布する。値X_1，X_2，…，X_nのうち、いくつかは等しい値であってもよい。上記式（１７）の計算は、有限体ＧＦ（ｑ）上で行われる。以降の説明においては、断りがない限り、演算は、有限体ＧＦ（ｑ）上で行われるものとする。

【００２９】

上記したような秘密分散法によりもとの秘密情報Ｓを分散した場合には、分散情報が配布されたメンバ全員（すなわちｎ人）が集まらない限り、もとの秘密情報Ｓを再構成することができない。もとの秘密情報Ｓは、次式（１８）を計算することにより、再構成できる。

$$S = X_1 + X_2 + \cdots + X_n \quad \cdots (18)$$

【００３０】

上記したような秘密分散法を、「加算秘密分散法」と呼ぶこととする。第１の実施形態は、上記した加算秘密分散法により秘密分散された分散情報を各メンバ

に配布し、各メンバが分散情報を所有している状態を前提とずる。もとの秘密情報Ｓを再構成させたいときに、集まったメンバ（ｎ人）が分散情報を持ち寄り、上記式（１８）を用いてもとの秘密情報Ｓを再構成することができるが、第１の実施形態に係る秘密再構成方法においては、この再構成時の計算を、マルチパーティ・プロトコルで分散計算することにより、集まった各メンバの分散情報を公開せずに、もとの秘密情報Ｓを再構成する。

【００３１】

第１の実施形態においては、複数のメンバからなるあるグループで、前述の秘密分散法（上記式（１７）による方法）を用いてもとの秘密情報Ｓから生成された分散情報が、各メンバに秘密裏に配布されている状態を前提とする。このグループにはｎ人のメンバがいるものとし、もとの秘密情報Ｓから生成され、各メンバに配布された分散情報をX_j（ｊ＝１，２，…，ｎ）とする。

【００３２】

第１の実施形態において、もとの秘密情報Ｓを再構成する際に、メンバ全員（すなわち、ｎ人のメンバ）が集まり、各メンバの持つ分散情報を持ち寄る。また、メンバのうち、どの２人のメンバ間にも、その２人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されているものとする。図３は、第１の実施形態において各メンバ間の通信に用いる秘密通信路３０３を示す図である。図３において、四角形で示されるブロックは集まったメンバを示し、m'_1，m'_2，…，m'_j，…，m'_tは、メンバＩＤを示し、両方向の矢印は、それぞれ対応するメンバ以外には通信内容を秘密とする秘密通信路３０３を示している。

【００３３】

次に、図４を用いて、第１の実施形態に係る秘密再構成方法の概要を説明する。図４においては、メンバの人数は３人（すなわち、演算記憶装置の数は３台）とし、各メンバは、もとの秘密情報Ｓを加算秘密分散法で分散させた分散情報Ａ，Ｂ，Ｃをそれぞれ持っているものとする。もとの秘密情報Ｓを再構成する場合には、まず、各メンバが持っている分散情報Ａ，Ｂ，Ｃを加算秘密分散法でさらに分散して、分散情報Ａ，Ｂ，Ｃの分散情報を生成する。具体的に言えば、図４

に符号①で示されるように、分散情報Ａを分散して分散情報Ａの分散情報Ａ１，Ａ２，Ａ３を生成し、分散情報Ｂを分散して分散情報Ｂの分散情報Ｂ１，Ｂ２，Ｂ３を生成し、分散情報Ｃを分散して分散情報Ｃの分散情報Ｃ１，Ｃ２，Ｃ３を生成する。次に、図４に符号②で示されるように、分散情報Ａ，Ｂ，Ｃの分散情報を他のメンバに配布する。図４に符号③で示されるように、各メンバは、分散情報Ａ，Ｂ，Ｃの分散情報Ａ１，Ｂ１，Ｃ１又はＡ２，Ｂ２，Ｃ２又はＡ３，Ｂ３，Ｃ３を受け取り、これらをもとに分散計算を行い、その分散計算の結果を出力する。次に、図４に符号④で示されるように、分散情報Ａ，Ｂ，Ｃの分散情報Ａ１，Ｂ１，Ｃ１と、Ａ２，Ｂ２，Ｃ２と、Ａ３，Ｂ３，Ｃ３とをそれぞれ用いて分散計算した計算結果を集めることにより、もとの秘密情報Ｓを再構成する。

【００３４】

図５は、本発明の第１の実施形態に係る秘密再構成方法を実施する構成（第１の実施形態に係る秘密再構成システム）を示すブロック図である。図５を用いて、第１の実施形態に係る秘密再構成方法を説明する。図５に示されるように、もとの秘密情報Ｓを再構成しようとする際に集まったｎ人のメンバ（すなわち、ｎ台の演算記憶装置）には、それぞれ、分散計算で秘密情報を再構成する手段である分散秘密再構成計算部（すなわち、第１の実施形態に係る分散秘密再構成装置）３０１（３０１－１，３０１－２，…，３０１－ｎ）が備えられている。ここで、符号３０１－ｊは、メンバｊ（ｊ＝１，２，…，ｎ）に備えられた分散秘密再構成計算部３０１を表わす。各メンバの分散秘密再構成計算部３０１－ｊ（ｊ＝１，２，…，ｎ）は、それぞれ他のメンバの分散秘密再構成計算部３０１と、図３で説明した秘密通信路３０３で接続されている。また、各メンバの分散秘密再構成計算部３０１－ｊ（ｊ＝１，２，…，ｎ）からの出力は、秘密再構成計算部３０２へ入力される。

【００３５】

秘密再構成計算部３０２は、各メンバの分散秘密再構成計算部３０１－ｊ（ｊ＝１，２，…，ｎ）からの出力を受け取り、それら受け取ったｎ個の値を、ｎ個の分散情報としたときの秘密情報の再構成を行う計算をし、その再構成された秘密情報を出力する。各メンバの分散秘密再構成計算部３０１－ｊ（ｊ＝１，２，

…，ｎ）から出力される値（すなわち、秘密再構成計算の中間計算結果）をＳｊ（ｊ＝１，２，…，ｎ）とすると、次式（１９）を用いて、もとの秘密情報Ｓを計算することができる。

【数７】

$$S = S_1 + S_2 + \cdots + S_n = \sum_{j=1}^{n} S_j \qquad (19)$$

上記式（１９）における各演算は有限体ＧＦ（ｑ）上で行う。なお、以降の説明においては、断りがない限り、演算は、有限体ＧＦ（ｑ）上で行われるものとする。

【００３６】

各メンバの分散秘密再構成計算部３０１－ｊ（ｊ＝１，２，…，ｎ）における処理は、各メンバが、それぞれ他のメンバにはその処理の内容が分からないように行う。秘密再構成計算部３０２における処理は、処理を統合するセンター（メンバとは別の演算装置）のようなものが行ってもよいし、集まったメンバ（演算記憶装置）のうちの１人、又は、複数人で行ってもよい。ただし、秘密情報Ｓを必要としているメンバが行うのが望ましい。

【００３７】

図６は、図５の分散秘密再構成計算部３０１－ｊ（ｊ＝１，２，…，ｎ）の構成を示すブロック図である。図６を用いて分散秘密再構成計算部３０１－ｊを説明する。図６に示されるように、分散秘密再構成計算部３０１－ｊは、秘密分散計算部４０１－ｊと、入力の数がｎ個である“（ｎ）加算部”４０２－ｊとを有する。秘密分散計算部４０１－ｊからの出力が“（ｎ）加算部”４０２－ｊへ入力され、“（ｎ）加算部”４０２－ｊからの出力が、分散秘密再構成計算部３０１－ｊの出力となる。

【００３８】

秘密分散計算部４０１－ｊへは、メンバｊが持っているもとの秘密情報Ｓの分散情報Ｘｊが入力される。秘密分散計算部４０１－ｊは、入力された分散情報Ｘｊを加算秘密分散法を用いて分散し、他のメンバと通信する秘密通信路３０３を

経由して配布する。分散情報X_jの分散情報$X_{j,n}$の計算は、$X_{j,1}$，$X_{j,2}$，…，$X_{j,n-1}$を、乱数として有限体ＧＦ（ｑ）上の値をｎ－１個選び、次式（２０）で、$X_{j,n}$求める。

$$X_{j,n}=X_j-(X_{j,1}+X_{j,2}+\cdots+X_{j,n-1}) \quad \cdots(20)$$

値$X_{j,1}$，$X_{j,2}$，…，$X_{j,n}$のうち、自分自身に対する分散情報$X_{j,j}$は、“（ｎ）加算部”４０２－ｊへ出力し、その他の分散情報$X_{j,p}$（ｐ＝１，２，…，ｎであり、ｐ≠ｊであるもの）は、秘密通信路３０３を通して各メンバに配布される。

【００３９】

“（ｎ）加算部”４０２－ｊは、秘密分散計算部４０１－ｊから、もとの秘密情報Ｓの分散情報X_jの分散情報$X_{j,j}$を受け取る。さらに、秘密通信路３０３を経由して、他のメンバから配布された、もとの秘密情報Ｓの分散情報X_p（ｐ＝１，２，…，ｎであり、ｐ≠ｊであるもの）の分散情報$X_{1,j}$，…，$X_{j-1,j}$，$X_{j+1,j}$，…，$X_{n,j}$を受け取る。これらｎ個ある、もとの秘密情報Ｓの分散情報の分散情報$X_{p,j}$（ｐ＝１，２，…，ｎ）から、もとの秘密情報Ｓの分散情報S_j（秘密情報Ｓの再構成時に得られる秘密情報Ｓの分散情報S_jと、秘密情報Ｓの分散時に得られる秘密情報Ｓの分散情報X_jとは異なるものである）を計算し出力する。“（ｎ）加算部”４０２－ｊは、次式（２１）のような計算を行い、秘密情報Ｓの分散情報S_jを出力する。

【数８】

$$S_j=X_{1,j}+X_{2,j}+\cdots+X_{n,j}=\sum_{p=1}^{n}X_{p,j} \quad (21)$$

【００４０】

[第１の実施形態の動作]

図７は、第１の実施形態に係る秘密再構成方法における動作を示すフローチャートである。ここで、もとの秘密情報Ｓを再構成するために集まったメンバ全員（ｎ人のメンバ）が持つ分散情報をX_1，X_2，…，X_nとする。

【００４１】

まず、各メンバが持つ分散情報X_1，X_2，…，X_nを加算秘密分散方法を用いて分散し、他のメンバに配布する（ステップＳ５０１）。ステップＳ５０１は、図６の秘密分散計算部４０１－ｊにおける動作を示しており、各メンバの持つ分散情報X_jから乱数生成及び上記式（２０）を用いて分散情報$X_{j,p}$（ｐ＝１，２，…，ｎ）を計算し、他のメンバに対して配布する。

【００４２】

次に、各メンバは、自分自身の分散情報X_jの分散情報及び他のメンバから配布された分散情報、すなわち、分散情報$X_{p,j}$（ｐ＝１，２，…，ｎ）を用いて演算を施し、もとの秘密情報Ｓの分散情報S_jを求める（ステップＳ５０２）。ステップＳ５０２は、図６の加算部４０２－ｊにおける動作を示しており、メンバｊは、他のメンバから配布された分散情報$X_{p,j}$（ｐ＝１，２，…，ｎ）（自分自身の分散情報X_jの分散情報$X_{j,j}$が含まれている）から、上記式（２１）を用いて計算する。その計算結果S_jは、もとの秘密情報Ｓの分散情報となっている。

【００４３】

次に、ステップＳ５０２で各メンバが計算した分散情報S_jからもとの秘密情報Ｓを再構成する（ステップＳ５０３）。ステップＳ５０３は、図５の秘密再構成計算部３０２における動作を示しており、メンバｊがステップＳ５０２で計算した結果S_j（ｊ＝１，２，…，ｎ）から、上記式（１９）を用いて計算し、もとの秘密情報Ｓを得ることができる。

【００４４】

[第１の実施形態の効果]

以上説明したように、第１の実施形態によれば、もとの秘密情報Ｓを再構成するために集まったメンバ（演算記憶装置）の持つ分散情報X_jを、他のメンバに公開せずに、もとの秘密情報Ｓを再構成することができる。したがって、各メンバが持つ分散情報X_jを、次回の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを設けなくても、上記の効果を達成することができる。また、第１の実施形態においては、分散情報Ｘ

$_j$を持つメンバ全員が集まらないと、もとの秘密情報S'を再構成することができないが、各メンバの匿名性は保たれており、さらに、秘密再構成の際のメンバ間の相互通信は、最初の分散情報を分散配布するための１回のみで済むため、通信量及び計算量の両方とも少ない。

【００４５】

さらに、秘密情報Ｓの分散情報X_jを持たない人（演算記憶装置）が、この再構成に参加しようとしても、秘密情報Ｓの再構成に失敗することから、第１の実施形態においては、集まった複数人数からなるグループ全員が正当メンバ（予め秘密情報Ｓの分散情報X_jを配布されたメンバ）か、そうでない人（演算記憶装置）が混在するか、ということを認証するような機能が備わる。さらにまた、第１の実施形態においては、前述したように分散情報を再利用可能なので、この認証機能は、秘密情報Ｓの分散情報を更新せずとも何度も利用できる。また、この認証機能は、集まったメンバから他へ送信される情報は、認証（秘密情報Ｓの再構成）のたびに異なるので、盗聴による“なりすまし”に非常に強い。このような認証機能は、秘密分散法の秘密再構成の性質と、マルチパーティ・プロトコルによる分散計算の性質との単なる組み合わせによって得られる機能ではなく、新しい機能である。なお、上記認証機能は、「もとの秘密情報Ｓ」を照合秘密情報Ｓ（予め登録されている情報で、認証が成立するか否かを、再構成結果と照らし合わせる情報）として用いる利用形態であるので、もとの秘密情報Ｓを各メンバに秘密にしない場合であっても、実現できる。

【００４６】

≪第２の実施形態≫

［第２の実施形態の概要］

本発明の第２の実施形態においては、もとの秘密情報Ｓを再構成する際に、もとの秘密情報Ｓを再構成するために集まったメンバ（演算記憶装置）が保有する分散情報を用いてマルチパーティ・プロトコルを実行することにより、各メンバが保有する分散情報を公開せずに、もとの秘密情報Ｓの再構成を行う。なお、第２の実施形態に係る秘密再構成方法は、秘密再構成システムにより実施される。第２の実施形態に係る秘密再構成システムは、各メンバ（演算記憶装置）である

分散秘密再構成装置（後述する分散秘密再構成計算部６０１）と、メンバのいずれかに又はメンバとは別のセンターに備えられた演算装置（後述する秘密再構成計算部６０２）とを主要な構成としている。

【００４７】

第１の実施形態は、複数のメンバからなるあるグループで、もとの秘密情報Ｓを、加算秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とした。これに対し、第２の実施形態は、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報Ｓを、（ｋ，ｎ）しきい値秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。第２の実施形態の場合には、必ずしもメンバ全員（すなわち、ｎ人のメンバ）が集まらなくとも、ｋ人（ｋ≦ｎ）のメンバが集まれば、もとの秘密情報Ｓを再構成することができる。

【００４８】

第２の実施形態においては、もとの秘密情報Ｓを再構成させたいときに、集まったメンバ（ｔ人、ｔ≧ｋ）が分散情報を持ち寄り、上記式（３）を用いてもとの秘密情報Ｓを再構成するが、この再構成時の計算を、マルチパーティ・プロトコルで分散計算することにより、集まった各メンバの分散情報を公開せずに、もとの秘密情報を再構成する。

【００４９】

［第２の実施形態の構成］

第２の実施形態は、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報Ｓを（ｋ，ｎ）しきい値秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。このグループにはｎ人のメンバがいるものとし、各メンバに秘密情報Ｓを分散させるときに用いたメンバＩＤをm_1，m_2，…，m_nとする。メンバＩＤがm_j（ｊ＝１，２，…，ｎ）であるメンバに配布した、秘密情報Ｓの分散情報をXm_j（ｊ＝１，２，…，ｎ）とする。もとの秘密情報Ｓを再構成させたいときに、集まったメンバがｔ人（ｔ≧ｋ）で、各メンバの持つ分散情報を持ち寄ったとする。このとき集まったメンバのメンバＩＤをm'_1，m'_2，…，m'_tとし、集まったメンバが持つ分散

情報をＸｍ’$_1$，Ｘｍ’$_2$，…，Ｘｍ’$_t$とする。また、集まったメンバのうち、どの２人のメンバ間にも、その２人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されているものとする。図３は、第２の実施形態において各メンバ間の通信に用いる秘密通信路３０３を示す図である。図３はおいて、四角形で示されるブロックは集まったメンバを示し、ｍ’$_1$，ｍ’$_2$，…，ｍ’$_j$，…，ｍ’$_t$は、メンバＩＤを示し、両方向の矢印は、それぞれ対応するメンバ以外には通信内容を秘密とする秘密通信路３０３を示している。さらに、集まったｔ人のメンバに与えられたメンバＩＤ＿ｍ’$_1$，ｍ’$_2$，…，ｍ’$_t$は公開された値であるものとする。

【００５０】

図８は、本発明の第２の実施形態に係る秘密再構成方法を実施する構成（第２の実施形態に係る秘密再構成システム）を示すブロック図である。図８を用いて、第２の実施形態に係る秘密再構成方法を説明する。図８に示されるように、もとの秘密情報Ｓを再構成しようとする際に集まったメンバＩＤがｍ’$_1$，ｍ’$_2$，…，ｍ’$_t$であるｔ人のメンバ（すなわち、ｔ台の演算記憶装置）は、それぞれ、分散計算により秘密情報を再構成する手段である分散秘密再構成計算部（すなわち、第２の実施形態に係る分散秘密再構成装置）６０１（６０１－１，６０１－２，…，６０１－ｔ）が備えられている。分散秘密再構成計算部６０１－ｊ（ｊ＝１，２，…，ｔ）における処理は、メンバＩＤがｍ’$_j$であるメンバが行う。各メンバの分散秘密再構成計算部６０１－ｊ（ｊ＝１，２，…，ｔ）は、それぞれ他のメンバの分散秘密再構成計算部６０１とは、図３で示された秘密通信路３０３で接続されている。また、各メンバの分散秘密再構成計算部６０１－ｊ（ｊ＝１，２，…，ｔ）からの出力は、秘密再構成計算部６０２へ入力される。分散秘密再構成計算部６０１及び秘密再構成計算部６０２は、第１の実施形態における分散秘密再構成計算部３０１及び秘密再構成計算部３０２と、構成及び動作において異なる点を持つ。

【００５１】

秘密再構成計算部６０２は、各メンバの分散秘密再構成計算部６０１－ｊ（ｊ＝１，２，…，ｔ）からの出力を受け取り、それら受け取ったｔ個の値を、ｔ個

の分散情報としたときの秘密情報の再構成を行う計算をし、その再構成された秘密情報を出力する。各メンバの分散秘密再構成計算部６０１－ｊ（ｊ＝１，２，…，ｔ）から出力される値をＳｍ’ｊ（ｊ＝１，２，…，ｔ）とすると、上記式（３）のＸｍ’ｊをＳｍ’ｊに置き換えた次式（２２）及び（４）を用いて計算し、もとの秘密情報Ｓを出力する。

【数９】

$$S = r_{m'_1} S_{m'_1} + r_{m'_2} S_{m'_2} + \cdots + r_{m'_t} S_{m'_t} = \sum_{j=1}^{t} r_{m'_j} S_{m'_j} \qquad (22)$$

$$r_{m'_j} = (m'_1 \times m'_2 \times \cdots \times m'_t / m'_j) / ((m'_1 - m'_j) \times (m'_2 - m'_j) \times \cdots \times (m'_{j-1} - m'_j) \times (m'_{j+1} - m'_j) \times \cdots \times (m'_t - m'_j)) = \prod_{\substack{i=1 \\ i \neq j}}^{t} m'_i / (m'_i - m'_j) \qquad (4)$$

上記式（２２）における各演算は有限体ＧＦ（ｑ）上で行う。以降の説明においては、断りがない限り、演算は、有限体ＧＦ（ｑ）上で行われるものとする。

【００５２】

各メンバの分散秘密再構成計算部６０１－ｊ（ｊ＝１，２，…，ｔ）における処理は、各メンバが、それぞれ他のメンバにはその処理の内容が分からないように行う。秘密再構成計算部６０２における処理は、処理を統合するセンター（メンバとは別の演算装置）のようなものが行ってもよいし、集まったメンバ（演算記憶装置）のうち、だれか１人、又は、複数人で行ってもよい。ただし、秘密情報Ｓを必要としているメンバが行うのが望ましい。

【００５３】

図９は、図８の分散秘密再構成計算部６０１－ｊ（ｊ＝１，２，…，ｔ）の構成を示すブロック図である。図９を用いて分散秘密再構成計算部６０１－ｊを説明する。図９に示されるように、分散秘密再構成計算部６０１－ｊは、秘密分散計算部７０１－ｊと、線形結合計算部７０２－ｊとを有する。秘密分散計算部７０１－ｊからの出力が線形結合計算部７０２－ｊへ入力され、線形結合計算部７

０２－ｊからの出力が、分散秘密再構成計算部７０１－ｊの出力となる。

【００５４】

秘密分散計算部７０１－ｊへは、メンバＩＤがm’ｊであるメンバが持つもとの秘密情報Ｓの分散情報Ｘm’ｊが入力される。秘密分散計算部７０１－ｊは、入力された分散情報Ｘm’ｊを（ｋ’，ｔ）しきい値秘密分散法（ｋ’≦ｔ）を用いて分散し、他のメンバと通信する秘密通信路３０３を経由して配布する。分散するときの計算においては、上記式（６）のｍｊがm’ｊに置き換わり、ｋがｋ’に置き換わったｋ’－１次多項式である次式（２３）を作る。

【数１０】

$$f m'_j(x)=Xm'_j+Rm'_{j,1}\,x+Rm'_{j,2}\,x^2+\cdots+Rm'_{j,k'-1}\,x^{k'-1} \qquad (23)$$

ここで、Ｒm’ｊ，１，Ｒm’ｊ，２，…，Ｒm’ｊ，ｋ’－１は、乱数として選ばれた有限体ＧＦ（ｑ）上のｋ’－１個の値である。

【００５５】

そして、メンバＩＤがm’ｐ（ｐ＝１，２，…，ｔ）であるメンバに対して配布する分散情報Ｘm’ｊ，ｐを、上記式（２３）を用いて次式（２４）のように計算する（上記式（７）参照）。

【数１１】

$$\begin{aligned} Xm'_{j,p} &= f m'_j(m'_p) \\ &= Xm'_j+Rm'_{j,1}(m'_p)+Rm'_{j,2}(m'_p)^2+\cdots+Rm'_{j,k'-1}(m'_p)^{k'-1} \end{aligned} \qquad (24)$$

【００５６】

自分自身に対する分散情報Ｘm’ｊ，ｊは、線形結合計算部７０２－ｊへ出力し、その他の分散情報Ｘm’ｊ，ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）を秘密通信路３０３を通して各メンバに配布する。

【００５７】

線形結合計算部７０２－ｊは、秘密分散計算部７０１－ｊから、もとの秘密情報Ｓの分散情報Ｘm’ｊの分散情報Ｘm’ｊ，ｊを受け取る。さらに、秘密通信路３０３を経由して、他のメンバから配布された、もとの秘密情報Ｓの分散情報Ｘ

m'jの分散情報Xm'1，j，…，Xm'j－1，j，Xm'j＋1，j，…，Xm't，jを受け取る。これらt個ある、もとの秘密情報Sの分散情報Xm'jの分散情報Xm'p，j（p＝1，2，…，t）、から、もとの秘密情報Sの分散情報Sm'j（秘密情報Sの再構成時に得られる秘密情報Sの分散情報Sm'jと、秘密情報Sの分散時に得られる秘密情報Sの分散情報Xm'jとは異なるものである）を計算し出力する。線形結合計算部７０２－jは、次式（２５）及び（２６）のような計算を行う。

【数１２】

$$Sm'_j = rm'_1\ Xm'_{1,j} + rm'_2\ Xm'_{2,j} + \cdots + rm'_t\ Xm'_{t,j}$$
$$= \sum_{p=1}^{t} rm'_p\ Xm'_{p,j} \qquad (25)$$

$$rm'_p = (m'_1 \times m'_2 \times \cdots \times m'_t / m'_p)$$
$$/((m'_1 - m'_p) \times (m'_2 - m'_p) \times \cdots \times (m'_{p-1} - m'_p) \times (m'_{p+1} - m'_p) \times$$
$$\cdots \times (m'_t - m'_p))$$
$$= \prod_{\substack{i=1 \\ i \neq p}}^{t} m'_i / (m'_i - m'_p) \qquad (26)$$

ここで、各メンバＩＤ__m'1，m'2，…，m'tは公開された値であるので、上記式（２６）のrm'pを計算することができる。

【００５８】

［第２の実施形態の動作］

図１０は、第２の実施形態に係る秘密再構成方法における動作を示すフローチャートである。ここで、もとの秘密情報Ｓを再構成するために集まったｔ人のメンバのメンバＩＤをm'1，m'2，…，m'tとし、各メンバが持つ分散情報をXm'1，Xm'2，…，Xm'tとする。

【００５９】

第２の実施形態に係る秘密再構成方法においては、図１０に示されるように、まず、各メンバが持つ分散情報を（k'，ｔ）しきい値秘密分散法を用いて分散し、他のメンバに配布する（ステップＳ８０１）。ステップＳ８０１は、図９の秘密分散計算部７０１－ｊにおける動作を示しており、メンバＩＤがm'j（ｊ

＝１，２，…，ｔ）であるメンバの持つ分散情報Ｘｍ’ｊを上記式（２３）を用いて分散し、メンバＩＤがｍ’ｐ（ｐ＝１，２，…，ｔ）であるメンバに対し、上記式（２４）で計算されるＸｍ’ｊ，ｐを配布する。

【００６０】

次に、各メンバは、公開されている集まったメンバのメンバＩＤ、自分自身の分散情報Ｘｍ’ｊの分散情報及び他のメンバから配布された分散情報、すなわち、分散情報Ｘｍ’ｐ，ｊ（ｐ＝１，２，…，ｔ）を用いて演算を施し、もとの秘密情報Ｓの分散情報Ｓｍ’ｊである値を求める（ステップＳ８０２）。ステップＳ８０２は、図９の線形結合計算部７０２－ｊにおける動作を示しており、メンバＩＤがｍ’ｊ（ｊ＝１，２，…，ｔ）であるメンバは、他のメンバから配布された分散情報Ｘｍ’ｐ，ｊ（ｐ＝１，２，…，ｔ）（自分自身の分散情報Ｘｍ’ｊの分散情報Ｘｍ’ｊ，ｊが含まれている）、及び公開されているメンバＩＤ＿ｍ’ｐ（ｐ＝１，２，…，ｔ）から、上記式（２５）を用いて計算する。その計算結果Ｓｍ’ｊは、もとの秘密情報Ｓの分散情報となっている。

【００６１】

次に、ステップＳ８０２で、各メンバが計算した分散情報からもとの秘密情報Ｓを再構成する（ステップＳ８０３）。ステップＳ８０３は、図８の秘密再構成計算部６０２における動作を示しており、メンバＩＤがｍ’ｊ（ｊ＝１，２，…，ｔ）であるメンバがステップＳ８０２で計算した結果Ｓｍ’ｊ（ｊ＝１，２，…，ｔ）から、上記式（２２）を用いて計算し、もとの秘密情報Ｓを得ることができる。

【００６２】

［第２の実施形態の効果］

以上説明したように、第２の実施形態によれば、第１の実施形態と同様に、もとの秘密情報Ｓを再構成するために集まったメンバの持つ分散情報を、他のメンバに公開せずに、もとの秘密情報Ｓを再構成することができる。したがって、各メンバが持つ分散情報を、次回の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを設けなくても、上記の効果を達成することができる。

【００６３】

また、上記第１の実施形態においては、もとの秘密情報Ｓは、各メンバに加算秘密分散法を用いて分散させていたので、メンバ全員が集まらないと、もとの秘密情報Ｓを再構成することができなかったが、第２の実施形態の場合、必ずしもメンバ全員、すなわちｎ人のメンバが集まらなくとも、ｋ人（ｋ≦ｎ）以上のメンバが集まれば、もとの秘密情報Ｓを再構成することができる。

【００６４】

このように、第２の実施形態においては、集まったメンバのメンバＩＤを公開するので、集まったメンバを匿名にすることはできないが（少なくとも、もとの秘密情報Ｓを秘密分散させるときのメンバＩＤは分かってしまうが）、秘密再構成の際のメンバ間の相互通信は、最初の分散情報を分散配布するための１回のみで済むため、通信量及び計算量の両方とも少なく、しかも、必ずしもメンバ全員、すなわちｎ人が集まらなくとも、ｋ人（ｋ≦ｎ）が集まれば、もとの秘密情報Ｓを再構成することができる。

【００６５】

さらに、第２の実施形態においては、第１の実施形態と同様に、予め秘密情報Ｓの分散情報を持たない人（演算記憶装置）が、この再構成に参加しようとしても、秘密情報Ｓの再構成に失敗することから、集まった複数人数からなるグループ全員が正当メンバ（予め秘密情報Ｓの分散情報を配布されたメンバ）か、そうでない人（演算記憶装置）が混在するか、ということを認証するような機能が備わる。さらにまた、第２の実施形態においては、前述のように分散情報を再利用可能なので、この認証機能は、秘密情報Ｓの分散情報を更新せずとも何度も利用できる。また、この認証機能は、集まったメンバから他へ送信される情報は、認証（秘密情報Ｓの再構成）のたびに異なるので、盗聴による“なりすまし”に非常に強い。このような認証機能は、秘密分散法の秘密再構成の性質と、マルチパーティ・プロトコルによる分散計算の性質との単なる組み合わせによって得られる機能ではなく、新しい機能である。なお、上記認証機能は、「もとの秘密情報Ｓ」を照合秘密情報Ｓ（予め登録されている情報で、認証が成立するか否かを、再構成結果と照らし合わせる情報）として用いる利用形態であるので、もとの秘

密情報Ｓを各メンバに秘密にしない場合であっても、実現できる。

【００６６】

≪第３の実施形態≫

［第３の実施形態の概要］

本発明の第３の実施形態においては、上記第１及び第２の実施形態と同様に、もとの秘密情報Ｓを再構成する際に、もとの秘密情報Ｓを再構成するために集まったメンバ（演算記憶装置）が保有する分散情報を用いてマルチパーティ・プロトコル（前述のマルチパーティ・プロトコルの第１方式）を実行することにより、各メンバが保有する分散情報を公開せずにもとの秘密情報Ｓの再構成を行う。なお、第３の実施形態に係る秘密再構成方法は、秘密再構成システムにより実施される。第３の実施形態に係る秘密再構成システムは、仮メンバＩＤ生成部（後述する図１２における符号９０１）と、各メンバ（演算記憶装置）である分散秘密再構成装置（後述する分散秘密再構成計算部９０２）と、メンバのいずれかに又はメンバとは別のセンターに備えられた演算装置（後述する秘密再構成計算部９０３）とを主要な構成としている。

【００６７】

第１の実施形態は、複数のメンバからなるあるグループで、もとの秘密情報Ｓを、加算秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提としていた。これに対し、第３の実施形態は、第２の実施形態と同様に、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報Ｓを、（ｋ，ｎ）しきい値秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。第３の実施形態の場合には、必ずしもメンバ全員（すなわち、ｎ人のメンバ）が集まらなくとも、ｋ人（ｋ≦ｎ）のメンバが集まれば、もとの秘密情報Ｓを再構成することができる。

【００６８】

また、上記第２の実施形態においては、集まったメンバのメンバＩＤを公開して秘密再構成を行っていたが、第３の実施形態においては、各メンバが保有する分散情報だけでなく、メンバＩＤをも公開せずに秘密情報の再構成を行なう。第３の実施形態においては、マルチパーティ・プロトコルは、前述したマルチパー

ティ・プロトコルの第１方式を使用する。

【００６９】

［第３の実施形態の構成］

第３の実施形態は、上記第２の実施形態と同様に、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報Ｓを（ｋ，ｎ）しきい値秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。このグループにはｎ人のメンバがいるものとし、各メンバに秘密情報Ｓを分散させるときに用いたメンバＩＤをm_1，m_2，…，m_nとする。メンバＩＤがm_j（ｊ＝１，２，…，ｎ）であるメンバに配布した、秘密情報Ｓの分散情報をXm_j（ｊ＝１，２，…，ｎ）とする。もとの秘密情報Ｓを再構成させたいときに、集まったメンバがｔ人（ｔ≧ｋ）で、各メンバの持つ分散情報を持ち寄ったとする。このとき集まったメンバのメンバＩＤをm'_1，m'_2，…，m'_tとし、そのメンバが持つ分散情報をXm'_1，Xm'_2，…，Xm'_tとする。また、上記第１及び第２の実施形態と同様に、集まったメンバのうち、どの２人のメンバ間にも、その２人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されているものとする（図３参照）。ただし、第２の実施形態とは異なり、集まったメンバのメンバＩＤ__m'_1，m'_2，…，m'_tは公開されず、どのメンバＩＤを持つメンバが集まっているかを知ることができないようになっている。また、以降の計算（加算「＋」及び乗算「×」などの四則演算）においては、有限体ＧＦ（ｑ）上の演算を行うものとする。

【００７０】

次に、図１１を用いて、第３の実施形態に係る秘密再構成方法の概要を説明する。図１１においては、メンバの人数は３人（すなわち、演算記憶装置の数は３台）とし、各メンバは、もとの秘密情報Ｓをしきい値秘密分散法で分散させた分散情報Xm_1，Xm_2，Xm_3及びメンバＩＤ__m_1，m_2，m_3をそれぞれ持っているものとする。もとの秘密情報Ｓを再構成する場合には、各メンバが持っている分散情報を、さらにしきい値秘密分散法で分散する。具体的に言えば、図１１に符号①で示されるように、秘密情報Ｓの分散情報Xm_1から秘密分散法により分散情報Xm_1の分散情報$Xm_{1,1}$，$Xm_{1,2}$，$Xm_{1,3}$を生成し、

秘密情報Ｓの分散情報Ｘｍ２から秘密分散法により分散情報Ｘｍ２の分散情報Ｘｍ２，１，Ｘｍ２，２，Ｘｍ２，３を生成し、秘密情報Ｓの分散情報Ｘｍ３から秘密分散法により分散情報Ｘｍ３の分散情報Ｘｍ３，１，Ｘｍ３，２，Ｘｍ３，３を生成する。さらに、メンバＩＤ＿ｍ１から秘密分散法によりメンバＩＤ＿ｍ１の分散情報ｍ１，１，ｍ１，２，ｍ１，３を生成し、メンバＩＤ＿ｍ２から秘密分散法によりメンバＩＤ＿ｍ２の分散情報ｍ２，１，ｍ２，２，ｍ２，３を生成し、メンバＩＤ＿ｍ３から秘密分散法によりメンバＩＤ＿ｍ３の分散情報ｍ３，１，ｍ３，２，ｍ３，３を生成する。そして、図１１に符号②で示されるように、秘密情報Ｓの分散情報Ｘｍ１，Ｘｍ２，Ｘｍ３の分散情報Ｘｍ１，１，Ｘｍ１，２，Ｘｍ１，３及びＸｍ２，１，Ｘｍ２，２，Ｘｍ２，３及びＸｍ３，１，Ｘｍ３，２，Ｘｍ３，３を他のメンバに配布する。次に、図１１に符号③で示されるように、各メンバは、受け取った分散情報の分散情報Ｘｍ１，１，Ｘｍ２，１，Ｘｍ３，１及びＸｍ１，２，Ｘｍ２，２，Ｘｍ３，２及びＸｍ１，３，Ｘｍ２，３，Ｘｍ３，３、並びに、メンバＩＤの分散情報ｍ１，１，ｍ２，１，ｍ３，１及びｍ１，２，ｍ２，２，ｍ３，２及びｍ１，３，ｍ２，３，ｍ３，３をもとに、分散計算行行い、その分散計算の結果を出力する。次に、図１１に符号④で示されるように、各メンバは、分散情報Ｘｍ１，１，Ｘｍ２，１，Ｘｍ３，１及びＸｍ１，２，Ｘｍ２，２，Ｘｍ３，２及びＸｍ１，３，Ｘｍ２，３，Ｘｍ３，３、並びに、分散情報ｍ１，１，ｍ２，１，ｍ３，１及びｍ１，２，ｍ２，２，ｍ３，２及びｍ１，３，ｍ２，３，ｍ３，３を用いた分散計算の計算結果を集めることにより、もとの秘密情報Ｓを再構成する。

【００７１】

図１２は、本発明の第３の実施形態に係る秘密再構成方法を実施する構成（第３の実施形態に係る秘密再構成システム）を示すブロック図である。図１２を用いて、第３の実施形態に係る秘密再構成方法を説明する。図１２に示されるように、もとの秘密情報Ｓを再構成しようとする際に集まったメンバＩＤがｍ’１，ｍ’２，…，ｍ’ｔであるメンバ（すなわち、ｔ台の演算記憶装置）は、それぞれ、分散計算により秘密情報を再構成する手段である分散秘密再構成計算部（すなわち、第３の実施形態に係る分散秘密再構成装置）９０２（９０２－１，９０２

－２，…，９０２－ｔ）が備えられている。また、秘密再構成方法を実施するシステムは、仮メンバＩＤ生成部９０１及び秘密再構成計算部９０３を有している。分散秘密再構成計算部９０２、及び秘密再構成計算部９０３は、第１及び第２の実施形態における分散秘密再構成計算部３０１及び６０１、並びに、秘密再構成計算部３０２及び６０２と、構成や動作に異なる点を持つ。仮メンバＩＤ生成部９０１は、集まった各メンバの分散秘密性構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）とそれぞれ接続されている。各メンバの分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）は、それぞれ他のメンバの分散秘密再構成計算部９０２とは、図３で説明した秘密通信路３０３で接続されている。また、各メンバの分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）からの出力は、秘密再構成計算部９０３へ入力される。

【００７２】

仮メンバＩＤ生成部９０１は、これら集まったメンバｔ人に対し、互いに重複した値をとらないようなｔ個の値d_1，d_2，…，d_tを生成し、これらの値を仮メンバＩＤとして、分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）へそれぞれ出力する。もし、ＩＰアドレスなどの互いに重複した値をとらないようなｔ個の値が既に利用できる状態であるならば、値を生成する代わりに、各分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）からそのような値を申請させて、それを仮メンバＩＤ＿d_1，d_2，…，d_tとして利用することもできる。さらに、これら仮メンバＩＤ＿d_1，d_2，…，d_tは公開され、それぞれがどの仮メンバＩＤを持つかは、集まった各メンバにとっては既知の値であるとする。その公開方法は、例えば、図１２に破線で示される制御信号を用いて、分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）が、仮メンバＩＤ＿d_j（ｊ＝１，２，…，ｔ）に対応しているかを通知する方法を採ることにより公開することもできる。仮メンバＩＤ生成部９０１は、仮メンバＩＤ＿d_1，d_2，…，d_tを各分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）に対応付け、仮メンバＩＤを公開する機能を持つ。

【００７３】

各メンバの分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）は、仮メ

ンバＩＤがｄｊであるメンバの処理部分であり、仮メンバＩＤ生成部９０１から、自分に対する仮メンバＩＤを受け取り、各自処理（詳細は後述）した出力結果と仮メンバＩＤ＿ｄｊを、秘密再構成計算部９０３へ出力する。

【００７４】

秘密再構成計算部９０３は、各メンバの分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）からの出力を受け取り、それら受け取ったｔ個の情報を、ｔ個の分散情報としたときの秘密情報の再構成を行う計算をし、その再構成された秘密情報を出力する。各メンバの分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）から出力される値をＳｄｊ（ｊ＝１，２，…，ｔ）及び仮メンバＩＤ＿ｄｊとすると、上記式（２２）及び（４）において、ｍ’ｊをｄｊに、Ｓｍ’ｊをＳｄｊに置き換えた次式（２７）及び（２８）を計算し、もとの秘密情報Ｓを出力する。

【数１３】

$$S = rd_1 Sd_1 + rd_2 Sd_2 + \cdots + rd_t Sd_t = \sum_{j=1}^{t} rd_j Sd_j \qquad (27)$$

$$rd_j = (d_1 \times d_2 \times \cdots \times d_t / d_j) / ((d_1 - d_j) \times (d_2 - d_j) \times \cdots \times (d_{j-1} - d_j) \times (d_{j+1} - d_j) \times \cdots \times (d_t - d_j)) = \prod_{\substack{i=1 \\ i \neq j}}^{t} d_i / (d_i - d_j) \qquad (28)$$

上記式（２７）及び（２８）における各演算は有限体ＧＦ（ｑ）上で行う。

【００７５】

各メンバの分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）における処理は、各メンバが、それぞれ他のメンバにはその処理の内容が分からないように行う。仮メンバＩＤ生成部９０１及び秘密再構成計算部９０３における処理は、処理を統合するセンター（メンバとは別の演算装置）のようなものが行ってもよいし、集まったメンバ（演算記憶装置）のうち、だれか１人、又は、複数人で行ってもよい。ただし、秘密再構成計算部９０３における処理は、秘密情報Ｓを必要としているメンバが行うのが望ましい。

【００７６】

図１３は、図１２の分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）の構成を示すブロック図である。図１３を用いて分散秘密再構成計算部９０２－ｊ（ｊ＝１，２，…，ｔ）を説明する。図１３に示されるように、分散秘密再構成計算部９０２－ｊは、秘密分散計算部１００１－ｊと、分散処理部１００２－ｊとを有する。分散秘密再構成計算部９０２－ｊへの入力は、秘密分散計算部１００１－ｊへ入力され、秘密分散計算部１００１－ｊからの出力が分散処理部１００２－ｊへ入力される。分散処理部１００２－ｊからの出力が、分散秘密再構成計算部９０２－ｊの出力となる。秘密分散計算部１００１－ｊには、図１２の仮メンバＩＤ生成部９０１から出力される仮メンバＩＤ＿ｄ$_j$が入力される。さらに、秘密分散計算部１００１－ｊには、仮メンバＩＤがｄ$_j$で与えられるメンバの持つメンバＩＤ＿ｍ’$_j$と、もとの秘密情報Ｓの分散情報Ｘｍ’$_j$とが入力される。秘密分散計算部１００１－ｊは、入力された分散情報Ｘｍ’$_j$及びメンバＩＤ＿ｍ’$_j$を、それぞれ（ｋ’，ｔ）しきい値秘密分散法を用いて分散し、他のメンバと通信する秘密通信路３０３を経由して配布する。第３の実施形態の場合には、第２の実施形態の場合とは異なり、分散乗算を行わなければならないので、この秘密分散法のしきい値ｋ’は、

$k' \leqq (t+1)/2$　　…（２９）

を満たさなければならない（上記式（１１）参照）。上記式（２９）の演算は、有限体ＧＦ（ｑ）上の演算ではなく、通常の実数、整数演算である。

【００７７】

入力された分散情報Ｘｍ’$_j$を分散するときの計算方法は、第２の実施形態と同様に、上記式（２３）のようなｋ’－１次多項式である次式（２９’）を作ることにより行う。

【数１４】

$$f_1 d_j(x) = Xm'_j + R_1 d_{j,1}\, x + R_1 d_{j,2}\, x^2 + \cdots + R_1 d_{j,k'-1}\, x^{k'-1} \qquad (29')$$

ただし、メンバＩＤ＿ｍ’$_p$（ｐ＝１，２，…，ｔ）は非公開の値であるので、代わりに仮メンバＩＤ＿ｄ$_p$（ｐ＝１，２，…，ｔ）を用いる。ここで、Ｒ$_1$ｄ

ｊ，１，Ｒ１ｄｊ，２，…，Ｒ１ｄｊ，ｋ’－１は、乱数として選ばれた有限体ＧＦ（ｑ）上のｋ’－１個の値である。

【００７８】

そして、仮メンバＩＤがｄｐ（ｐ＝１，２，…，ｔ）であるメンバに対して配布する分散情報Ｘｍ’ｊ，ｐを、上記式（２９’）を用いて次式（３０）のように計算する。

【数１５】

$$Xm'_{j,p}=f_1d_j(d_p)$$
$$=Xm'_j+R_1d_{j,1}(d_p)+R_1d_{j,2}(d_p)^2+\cdots+R_1d_{j,k'-1}(d_p)^{k'-1} \quad (30)$$

【００７９】

入力されるメンバＩＤ＿ｍ’ｊを分散するときは、同様に、次式（３１）なるｋ’－１次多項式を作る。

【数１６】

$$f_2d_j(x)=m'_j+R_2d_{j,1}\,x+R_2d_{j,2}\,x^2+\cdots+R_2d_{j,k'-1}\,x^{k'-1} \quad (31)$$

ここで、Ｒ２ｄｊ，１，Ｒ２ｄｊ，２，…，Ｒ２ｄｊ，ｋ’－１は、乱数として選ばれた有限体ＧＦ（ｑ）上のｋ’－１個の値である。

【００８０】

そして、仮メンバＩＤがｄｐ（ｐ＝１，２，…，ｔ）であるメンバに対して配布する分散情報ｍ’ｊ，ｐを、上記式（３１）を用いて次式（３２）のように計算する。

【数１７】

$$m'_{j,p}=f_2d_j(d_p)$$
$$=m'_j+R_2d_{j,1}(d_p)+R_2d_{j,2}(d_p)^2+\cdots+R_2d_{j,k'-1}(d_p)^{k'-1} \quad (32)$$

【００８１】

自分自身に対する分散情報Ｘｍ’ｊ，ｊ及びｍ’ｊ，ｊは、分散処理部１００２－ｊへ出力し、その他の分散情報Ｘｍ’ｊ，ｐ及びｍ’ｊ，ｐ（ｐ＝１，２，…，ｔで

あり、ｐ≠ｊであるもの）を秘密通信路３０３を通して各メンバに配布する（他のメンバの分散処理部１００２－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）へ送信する）。

【００８２】

分散処理部１００２－ｊは、秘密分散計算部１００１－ｊから、メンバＩＤの分散情報$m'_{j,j}$、及び、もとの秘密情報Ｓの分散情報の分散情報$Xm'_{j,j}$を受け取る。さらに、秘密通信路３０３を経由して、他のメンバから配布された（他のメンバの秘密分散計算部１００１－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）から送信された）、他のメンバのメンバＩＤの分散情報$m'_{1,j}$，$m'_{2,j}$，…，$m'_{t,j}$、及び、もとの秘密情報Ｓの分散情報の分散情報である$Xm'_{1\cdot j}$，$Xm'_{2\cdot j}$，…，$Xm'_{t\cdot j}$を受け取る。これらメンバＩＤの分散情報$m'_{p,j}$（ｐ＝１，２，…，ｔ）と、もとの秘密情報Ｓの分散情報の分散情報$Xm'_{p,j}$（ｐ＝１，２，…，ｔ）、から、もとの秘密情報Ｓの分散情報となるSd_jを計算して出力する。すなわち、集まったメンバのメンバＩＤ__m'_1，m'_2，…，m'_t及び分散情報Xm'_1，Xm'_2，…，Xm'_tを分散させたまま、上記式（３）で示される式の分散計算を行う。その結果得られる値Ｓは、分散秘密情報Sd_1，Sd_2，…，Sd_tとして、各メンバがそれぞれ持っていることになる。

【００８３】

図１４は、図１３の分散処理部１００２－ｊ（ｊ＝１，２，…，ｔ）の構成を示すブロック図である。図１４を用いて分散処理部１００２－ｊ（ｊ＝１，２，…，ｔ）の構成を説明する。分散処理部１００２－ｊは、ｔ個の項計算部１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）と、ｔ個の情報が入力される“（ｔ）加算部”１１０２－ｊとを有する。秘密分散計算部１００１－ｊからの出力$Xm'_{j,j}$及び$m'_{j,j}$、さらに、秘密通信路３０３を経由して、他のメンバから配布された（他のメンバの秘密分散計算部１００１－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）から送信された）、他のメンバのメンバＩＤの分散情報$m'_{1,j}$，$m'_{2,j}$，…，$m'_{t,j}$、及び、もとの秘密情報Ｓの分散情報の分散情報$Xm'_{1,j}$，$Xm'_{2,j}$，…，$Xm'_{t,j}$は、項計算部１１０１－ｊ－ａ

（ａ＝１，２，…，ｔ）へ入力される。項計算部１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）からの出力は、“（ｔ）加算部”１１０２－ｊへ入力され、“（ｔ）加算部”１１０２－ｊからの出力が、分散処理部１００２－ｊの出力となる。項計算部１１０１－ｊ－ａは、それぞれ、他のメンバの秘密分散計算部１００１－ｐ及び項計算部１１０１－ｐ－ａ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）との秘密通信路３０３を持っている。

【００８４】

“（ｔ）加算部”１１０２－ｊは、項計算部１１０１－１－ａ（ａ＝１，２，…，ｔ）からそれぞれ一つずつの出力（合計ｔ個）を受け取り、それらをすべて（ｔ個）加算する。すなわち、項計算部１１０１－ｊ－ａからの出力をY_a（ａ＝１，２，…，ｔ）とすると、“（ｔ）加算部”１１０２－ｊは、次式（３３）、すなわち、

$$Sd_j = Y_1 + Y_2 + \cdots + Y_t \quad \cdots (33)$$

を計算し、計算結果であるSd_jを出力する。

【００８５】

図１５は、図１４の項計算部１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）の構成を示すブロック図である。次に、図１５を用いて項計算部１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）の構成を説明する。項計算部１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）は、差分計算部１２０１－ｊ－ａと、ｔ－１個の情報が入力される“（ｔ－１）分散乗算部”１２０２－ｊ－ａと、ｔ－１個の情報が入力される“（ｔ－１）分散乗算部”１２０４－ｊ－ａと、分散逆元計算部１２０３－ｊ－ａと、２個の情報が入力される“（２）分散乗算部”１２０５－ｊ－ａと、２個の情報が入力される“（２）分散乗算部”１２０６－ｊ－ａとを有する。項計算部１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）へ入力される$m'_{1,j}$，$m'_{2,j}$，…，$m'_{t,j}$は、秘密通信路３０３を通して、差分計算部１２０１－ｊ－ａへ入力され（ただし、$m'_{j,j}$は、秘密分散計算部１００１－ｊからの入力）、差分計算部１２０１－ｊ－ａからの出力は、“（ｔ－１）分散乗算部”１２０２－ｊ－ａへ入力される。“（ｔ－１）分散乗算部”１２０２－ｊ－ａからの出力は、分散逆元計算部１２０３－ｊ－ａへ入力され、分散逆元計算部１２０３－ｊ－ａ

からの出力は、“（２）分散乗算部”１２０５－ｊ－ａへ入力される。また、項計算部１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）へ秘密通信路３０３を通して入力されるｍ’１，ｊ，ｍ’２，ｊ，…，ｍ’ｔ，ｊ（ただし、ｍ’ｊ，ｊは、秘密分散計算部１００１－ｊからの入力）のうちｍ’ａ，ｊ以外の値は、“（ｔ－１）分散乗算部”１２０４－ｊ－ａへも入力され、“（ｔ－１）分散乗算部”１２０４－ｊ－ａからの出力は、分散逆元計算部１２０３－ｊ－ａからの出力とともに、“（２）分散乗算部”１２０５－ｊ－ａへ入力される。“（２）分散乗算部”１２０５－ｊ－ａからの出力は、項計算部１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）へ秘密通信路３０３を通して入力されるＸｍ’ａ，ｊ（ただし、項計算部１１０１－ｊ－ｊへの入力Ｘｍ’ｊ，ｊは、秘密分散計算部１００１－ｊからの入力）とともに、“（２）分散乗算部”１２０６－ｊ－ａへ入力される。“（２）分散乗算部”１２０６－ｊ－ａからの出力が、項計算部１１０１－ｊ－ａの出力となる。また、“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａ、分散逆元計算部１２０３－ｊ－ａ、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａはそれぞれ、他のメンバの、“（ｔ－１）分散乗算部”１２０２－ｐ－ａ，１２０４－ｐ－ａ、分散逆元計算部１２０３－ｐ－ａ、“（２）分散乗算部”１２０５－ｐ－ａ，１２０６－ｐ－ａ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）との秘密通信路３０３を持っている。

【００８６】

差分計算部１２０１－ｊ－ａは、項計算部１１０１－ｊ－ａへ入力されるメンバＩＤ＿ｍ’１，ｊ，ｍ’２，ｊ，…，ｍ’ｔ，ｊを受け取り、それぞれのメンバＩＤ＿ｍ’１，ｊ，ｍ’２，ｊ，…，ｍ’ｔ，ｊとｍ’ａ，ｊの差分を計算する。ただし、ｍ’ａ，ｊ同士の差分は計算しない。すなわち、（ｍ’１，ｊ－ｍ’ａ，ｊ），（ｍ’２，ｊ－ｍ’ａ，ｊ），…，（ｍ’（ａ－１），ｊ－ｍ’ａ，ｊ），（ｍ’（ａ＋１），ｊ－ｍ’ａ，ｊ），…，（ｍ’ｔ，ｊ－ｍ’ａ，ｊ）のｔ－１個の差分の計算を行う。これらｔ－１個の計算結果は、“（ｔ－１）分散乗算部”１２０２－ｊ－ａへ出力される。

【００８７】

“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａは、内部的に

は同じ構成であり、ｔ－１個の入力を受け取り、それらの入力と秘密通信路３０３からの情報を用いて、ｔ－１個の要素の分散乗算を行い、その計算結果を出力する。“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａへ入力される値を$A_{1,j}$，$A_{2,j}$，…，$A_{(t-1),j}$とする。$A_{i,j}$（ｉ＝１，２，…，ｔ－１）と、他のメンバの“（ｔ－１）分散乗算部”１２０２－ｐ－ａ，１２０４－ｐ－ａへ入力される$A_{i,p}$（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）の、ｔ個の値$A_{i,p}$（ｐ＝１，２，…，ｔ）を分散情報として再構成されるようなもとの秘密をA_iとすると、“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａは、A_i（ｉ＝１，２，…，ｔ－１）をすべて乗算した値

$B=A_1\times A_2\times\cdots\times A_{t-1}$

の、仮メンバＩＤがd_jであるメンバに対する分散情報B_jを計算することとなる。“（ｔ－１）分散乗算部”１２０２－ｊ－ａは、差分計算部１２０１－ｊ－ａからのｔ－１個の出力を受け取り、それらを用いて計算し、その計算結果を分散逆元計算部１２０３－ｊ－ａへ出力する。“（ｔ－１）分散乗算部”１２０２－ｊ－ａは、他のメンバの“（ｔ－１）分散乗算部”１２０２－ｐ－ａ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）と秘密通信路３０３を経由して必要な情報をやり取りする。“（ｔ－１）分散乗算部”１２０４－ｊ－ａは、項計算部１１０１－ｊ－ａへ入力されるｍ’１，ｊ，ｍ’２，ｊ，…，ｍ’ｔ，ｊのうち、ｍ’ａ，ｊ以外のものを受け取り、それらを用いて計算し、その計算結果を“（２）分散乗算部”１２０５－ｊ－ａへ出力する。“（ｔ－１）分散乗算部”１２０４－ｊ－ａは、他のメンバの“（ｔ－１）分散乗算部”１２０４－ｐ－ａ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）と秘密通信路３０３を経由して必要な情報をやり取りする。

【００８８】

分散逆元計算部１２０３－ｊ－ａは、“（ｔ－１）分散乗算部”１２０２－ｊ－ａからの出力を受け取り、その値と秘密通信路３０３からの情報を用いて分散計算し、その計算結果を、“（２）分散乗算部”１２０５－ｊ－ａへ出力する。分散逆元計算部１２０３－ｊ－ａへ入力される値をA_jとし、この入力A_jと他

のメンバの分散逆元計算部１２０３－ｐ－ａへ入力されるＡ$_{p}$（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）の、ｔ個の値Ａ$_{p}$（ｐ＝１，２，…，ｔ）を分散情報としてを再構成されるようなもとの秘密Ａとすると、分散逆元計算部１２０３－ｊ－ａは、Ａの有限体ＧＦ（ｑ）上の逆元Ｂ＝Ａ$^{-1}$の、仮メンバＩＤがｄ$_{j}$であるメンバに対する分散情報Ｂ$_{j}$を計算することとなる。分散逆元計算部１２０３－ｊ－ａは、他のメンバの分散逆元計算部１２０３－ｐ－ａ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）と秘密通信路３０３を経由して必要な情報をやり取りする。

【００８９】

“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａは、内部的には同じ構成であり、２個の入力を受け取り、それらの入力と秘密通信路３０３からの情報を用いて、２個の要素の分散乗算を行い、その計算結果を出力する。“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａへ入力される値をＡ$_{1,j}$，Ａ$_{2,j}$とする。Ａ$_{i,j}$（ｉ＝１，２）と、他のメンバの“（２）分散乗算部”１２０５－ｐ－ａ，１２０６－ｐ－ａへ入力されるＡ$_{i,p}$（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）の、２個の値Ａ$_{i,p}$（ｐ＝１，２，…，ｔ）を分散情報として再構成されるようなもとの秘密をＡ$_{i}$（ｉ＝１，２）とすると、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａは、Ａ$_{1}$及びＡ$_{2}$を乗算した値Ｂ＝Ａ$_{1}$×Ａ$_{2}$の、仮メンバＩＤがｄ$_{j}$であるメンバに対する分散情報Ｂ$_{j}$を計算することとなる。“（２）分散乗算部”１２０５－ｊ－ａは、“（ｔ－１）分散乗算部”１２０４－ｊ－ａ及び分散逆元計算部１２０３－ｊ－ａからの出力を受け取り、それらを用いて計算し、その計算結果を“（２）分散乗算部”１２０６－ｊ－ａへ出力する。“（２）分散乗算部”１２０５－ｊ－ａは、他のメンバの“（２）分散乗算部”１２０５－ｐ－ａ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）と秘密通信路３０３を経由して必要な情報をやり取りする。“（２）分散乗算部”１２０６－ｊ－ａは、“（２）分散乗算部”１２０５－ｊ－ａからの出力、及び、項計算部１１０１－ｊ－ａへ入力されるＸｍ’ａ，ｊを受け取り、それらを用いて計算し、その計算結果を出力する。“（２）分散乗算部”１２０６－ｊ－ａは、他のメンバの“（２）分散乗算部”１２０６

－ｐ－ａ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）と秘密通信路３０３を経由して必要な情報をやり取りする。

【００９０】

図１６は、図１５の“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａ（ｊ＝１，２，…，ｔ、ａ＝１，２，…，ｔ）の構成を示すブロック図である。図１６を用いて“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａ（ｊ＝１，２，…，ｔ、ａ＝１，２，…，ｔ）の構成を説明する。ここで、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａへ入力される２つの入力をそれぞれ、Ａｄｊ及びＢｄｊとし、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａからの出力をＣｄｊとする。“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａは、乗算部１３０１－ｊと、秘密分散計算部１３０２－ｊと、線形結合計算部１３０３－ｊとを有する。“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａへ入力されるＡｄｊ及びＢｄｊは、乗算部１３０１－ｊへ入力され、乗算部１３０１－ｊからの出力は、秘密分散計算部１３０２－ｊへ入力され、さらに、秘密分散計算部１３０２－ｊからの出力は、線形結合計算部１３０３－ｊへ入力される。線形結合計算部１３０３－ｊからの出力が、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａからの出力となる。

【００９１】

乗算部１３０１－ｊは、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａへ入力されるＡｄｊ及びＢｄｊを受け取り、それらを乗算する。すなわち、

$$C'd_j = Ad_j \times Bd_j \quad \cdots(34)$$

を計算して、その計算結果Ｃ’ｄｊを、秘密分散計算部１３０２－ｊへ出力する。

【００９２】

秘密分散計算部１３０２－ｊは、第２の実施形態における図９の秘密分散計算部７０１－ｊと内部的には同じ構成であり、入力される値を（ｋ’，ｔ）しきい値秘密分散法を用いて分散して出力する。前述の通り、第３の実施形態の場合、分散乗算を行わなければならないので、この秘密分散法のしきい値ｋ’は、

$k' \leqq (t+1)/2$　　…（２９）

を満たさなければならない。ここで、式（２９）の演算は、有限体ＧＦ（ｑ）上の演算ではなく、通常の実数、整数演算である。

【００９３】

また、分散に用いるときのメンバＩＤ__m'_1，m'_2，…，m'_tは非公開なので、第３の実施形態においては、仮メンバＩＤ__d_1，d_2，…，d_tを用いる。今、秘密分散計算部１３０２－ｊへ入力される値は$C'd_j$なので、次式（３５）のｋ’－１次多項式を作り、$R_3d_{j,1}$，$R_3d_{j,2}$，…，$R_3d_{j,k'-1}$は、乱数として有限体ＧＦ（ｑ）上の値をｋ’－１個選ぶ。

【数１８】

$$f_3d_j(x)=C'd_j+R_3d_{j,1}\,x+R_3d_{j,2}\,x^2+\cdots+R_3d_{j,k'-1}\,x^{k'-1} \qquad (35)$$

【００９４】

仮メンバＩＤがd_p（ｐ＝１，２，…，ｔ）であるメンバに対して配布する分散情報$C'd_{j,p}$を、上記式（３５）を用いて次式（３６）のように計算する。

【数１９】

$$\begin{aligned} C'd_{j,p} &= f_3d_j(d_p) \\ &= C'd_j+R_3d_{j,1}(d_p)+R_3d_{j,2}(d_p)^2+\cdots+R_3d_{j,k'-1}(d_p)^{k'-1} \end{aligned} \qquad (36)$$

【００９５】

自分自身に対する分散情報$C'd_{j,j}$は、線形結合計算部１３０３－ｊへ出力し、その他の分散情報$C'd_{j,p}$（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）を秘密通信路３０３を通して各メンバに配布する（他のメンバの線形結合計算部１３０３－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）へ送信する）。

【００９６】

線形結合計算部１３０３－ｊは、第２の実施形態における図９の線形結合計算部７０２－ｊと内部的には同じ構成であるが、計算に用いるメンバＩＤ__m'_1

，ｍ’２，…，ｍ’ｔは非公開なので、第３の実施形態においては、仮メンバＩＤ＿ｄ１，ｄ２，…，ｄｔを用いる。線形結合計算部１３０３－ｊは、秘密分散計算部１３０２－ｊから、分散情報Ｃ’ｄｊ，ｊを受け取る。さらに、秘密通信路３０３を経由して、他のメンバの秘密分散計算部１３０２－ｉ（ｉ＝１，２，…，ｔでｉ≠ｊであるもの）から配布された分散情報Ｃ’ｄ１，ｊ，Ｃ’ｄ２，ｊ，…，Ｃ’ｄｔ，ｊを受け取る。線形結合計算部１３０３－ｊは、これら全部でｔ個ある分散情報Ｃ’ｄｐ，ｊ（ｐ＝１，２，…，ｔ）、から、次式（３７）及び（３８）のような計算を行い、出力となるＣｄｊを算出する。

【数２０】

$$Cd_j = rd_1 C'd_{1,j} + rd_2 C'd_{2,j} + \cdots + rd_t C'd_{t,j} = \sum_{p=1}^{t} rd_p C'd_{p,j} \qquad (37)$$

$$rd_p = (d_1 \times d_2 \times \cdots \times d_t / d_p) / ((d_1 - d_p) \times (d_2 - d_p) \times \cdots \times (d_{p-1} - d_p) \times (d_{p+1} - d_p) \times \cdots \times (d_t - d_p)) = \prod_{\substack{i=1 \\ i \neq p}}^{t} d_i / (d_i - d_p) \qquad (38)$$

各仮メンバＩＤ＿ｄ１，ｄ２，…，ｄｔは公開され、既知の値であるので式（３８）のｒｄｐを計算することができる。

【００９７】

図１７は、図１５の“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａ（ｊ＝１，２，…，ｔ；ａ＝１，２，…，ｔ）の構成を示すブロック図である。図１７を用いて“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａ（ｊ＝１，２，…，ｔ、ａ＝１，２，…，ｔ）の構成を説明する。今、“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａへ入力されるｔ－１個の入力をＡ１，Ａ２，…，Ａｔ－１とする。“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａは、ｔ－２個の“（２）分散乗算部”１４０１－ｉ（ｉ＝１，２，…，ｔ－２）を有する。ｔ－２個の“（２）分散乗算部”１４０１－ｉ（ｉ＝１，２，…，ｔ－２）は、“（２）分散乗算部”１４０１－ｉからの出力が次の“（２）分散乗算部”１４０１－（ｉ＋１）への入力の一つとなるように、多段に構成されている。“（ｔ－１）分散乗算部”１２０２－ｊ－

ａ，１２０４－ｊ－ａへ入力される２つの入力Ａ$_1$及びＡ$_2$は、“（２）分散乗算部”１４０１－１へ入力され、“（２）分散乗算部”１４０１－１からの出力は、次の“（２）分散乗算部”１４０１－２へ、“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａへ入力されるＡ$_3$とともに、入力される。“（２）分散乗算部”１４０１－ｉ（ｉ＝２，…，ｔ－２）へは、“（２）分散乗算部”１４０１－（ｉ－１）からの出力が、“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａへ入力されるＡ（ｉ＋１）とともに、入力され、“（２）分散乗算部”１４０１－ｉ（ｉ＝１，…，ｔ－３）からの出力は、“（２）分散乗算部”１４０１－（ｉ＋１）に入力される。“（２）分散乗算部”１４０１－（ｔ－２）からの出力が、“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａからの出力となる。

【００９８】

“（２）分散乗算部”１４０１－ｉ（ｉ＝１，２，…，ｔ－２）は、前に説明した、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａと同じ構成をしている。“（２）分散乗算部”１４０１－ｉ（ｉ＝１，２，…，ｔ－２）は、他のメンバの“（２）分散乗算部”１４０１－ｉ（ｉ＝１，２，…，ｔ－２）とそれぞれ秘密通信路３０３を通して通信を行う。

【００９９】

図１８は、図１５の分散逆元計算部１２０３－ｊ－ａ（ｊ＝１，２，…，ｔ、ａ＝１，２，…，ｔ）の構成を示すブロック図である。図１８を用いて分散逆元計算部１２０３－ｊ－ａ（ｊ＝１，２，…，ｔ、ａ＝１，２，…，ｔ）の構成を説明する。分散逆元計算部１２０３－ｊ－ａは、ｑ$_b$－１個の“（２）分散乗算部”１５０１－ｉ（ｉ＝１，２，…，ｑ$_b$－１）と、乗算制御部１５０２と、“（ｑ$_b$）分散乗算部”１５０３とを有する。ｑ$_b$は、第３の実施形態において前提としている有限体ＧＦ（ｑ）の要素数ｑから２を引いた値の底２における対数をとった値（小数点以下切り上げ）であり、次式（３９）のように計算できる。

$$q_b = ceil(\log_2(q-2)) \quad \cdots(39)$$

【０１００】

ここで、ｃｅｉｌ（・）は、小数点以下切り上げの演算を表し、ｌｏｇ$_2$（・

）は、底２の対数をとることを表す。上記式（３９）の演算は、有限体ＧＦ（ｑ）上の演算ではなく、通常の実数、整数演算である。今、分散逆元計算部１２０３－ｊ－ａへの入力をＡｊとすると、この入力Ａｊと他のメンバの分散逆元計算部１２０３－ｐ－ａへ入力されるＡｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）の、ｔ個の値Ａｐ（ｐ＝１，２，…，ｔ）を分散情報としてを再構成されるようなもとの秘密Ａとする。この場合、分散逆元計算部１２０３－ｊ－ａは、Ａの有限体ＧＦ（ｑ）上の逆元Ｂ＝Ａ－１の、仮メンバＩＤがｄｊであるメンバに対する分散情報Ｂｊを計算して出力することとなる。有限体の性質により、有限体ＧＦ（ｑ）上の演算においては、有限体ＧＦ（ｑ）のある要素Ａに対して、次式（４０）、すなわち、

Ａ－１＝Ａｑ－２　　…（４０）

が成立するので、分散逆元計算部１２０３－ｊ－ａにおいては、Ａｊをｑ－２回分散乗算する計算を行う。

【０１０１】

ｑｂ－１個の“（２）分散乗算部”１５０１－ｉ（ｉ＝１，２，…，ｑｂ－１）は、“（２）分散乗算部”１５０１－ｉからの出力が次の“（２）分散乗算部”１５０１－（ｉ＋１）への両方の入力となっているように、多段に構成されている。分散逆元計算部１２０３－ｊ－ａへ入力される入力Ａｊは、“（２）分散乗算部”１５０１－１へ入力され、“（２）分散乗算部”１５０１－１からの出力は、次の“（２）分散乗算部”１５０１－２へ入力される。分散逆元計算部１２０３－ｊ－ａへ入力される入力Ａｊ、及び各“（２）分散乗算部”１５０１－ｉ（ｉ＝１，２，…，ｑｂ－１）からの出力の、合計ｑｂ個の値は、乗算制御部１５０２へ入力され、乗算制御部１５０２から出力される値は、“（ｑｂ）分散乗算部”１５０３へ入力される。“（ｑｂ）分散乗算部”１５０３からの出力が分散逆元計算部１２０３－ｊ－ａからの出力となる。

【０１０２】

“（２）分散乗算部”１５０１－ｉ（ｉ＝１，２，…，ｑｂ－１）は、前に説明した、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａと同じ構成をしている。“（２）分散乗算部”１５０１－ｉ（ｉ＝１，２，…，ｑｂ－１）

は、他のメンバの“（２）分散乗算部”１５０１－ｉ（ｉ＝１，２，…，ｑｂ－１）とそれぞれ秘密通信路３０３を通して通信を行う。

【０１０３】

乗算制御部１５０２は、分散逆元計算部１２０３－ｊ－ａへ入力される入力Ａｊ及び各“（２）分散乗算部”１５０１－ｉ（ｉ＝１，２，…，ｑｂ－１）からの出力の、合計ｑｂ個の値を受け取り、入力されたｑｂ個の値を、そのまま出力するか、又は、１を出力する、ということを制御する。入力されたそれぞれの値をどう出力するかは、次のようなルールで行う。まず、“（２）分散乗算部”１５０１－ｉ（ｉ＝１，２，…，ｑｂ－１）からの出力をＡｊ，ｉ＋１とする。乗算制御部１５０２へは、ｑｂ個の値Ａｊ，ｉ（ｉ＝１，２，…，ｑｂ）が入力されることとなる（ただし、Ａｊ，１＝Ａｊ）。また、ｑ－２を２進数表現し、そのときの各桁の値を大きい桁からｂｑｂ，ｂ（ｑｂ－１），…，ｂ２，ｂ１とする（ｑ－２は、ｑｂ桁の２進数で表すことができる）。乗算制御部１５０２は、上記ｂｉ（ｉ＝１，２，…，ｑｂ）が１であるならば値Ａｊ，ｉを出力し、上記ｂｉ（ｉ＝１，２，…，ｑｂ）が０であるならば値１を出力する。出力されたｑｂ個の値は、“（ｑｂ）分散乗算部”１５０３へ入力される。

【０１０４】

“（ｑｂ）分散乗算部”１５０３は、前述した“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａと同様な構成をしているが、“（２）分散乗算部”がｔ－２個ではなく、ｑｂ－１個になっている構成である。“（ｑｂ）分散乗算部”１５０３は、他のメンバの“（ｑｂ）分散乗算部”１５０３とそれぞれ秘密通信路３０３を通して通信を行う。

【０１０５】

[第３の実施形態の動作]

図１９は、第３の実施形態に係る秘密再構成方法における動作を示すフローチャートである。ここで、もとの秘密情報Ｓを再構成するために集まったｔ人のメンバのメンバＩＤをｍ’１、ｍ’２，…，ｍ’ｔとし、各メンバが持つ分散情報をＸｍ’１，Ｘｍ’２，…，Ｘｍ’ｔとする。

【０１０６】

図１９に示されるように、まず、集まった各メンバに対して、分散計算時に用いる仮メンバＩＤを割り当てるために、仮メンバＩＤ＿ｄ$_1$，ｄ$_2$，…，ｄ$_t$を生成し、各メンバに配布、そして、公開する（ステップＳ１６０１）。ステップＳ１６０１は、図１２の仮メンバＩＤ生成部９０１における動作を示しており、各メンバに重複なく仮メンバＩＤ＿ｄ$_1$，ｄ$_2$，…，ｄ$_t$を割り当て、配布、公開する。

【０１０７】

次に、各メンバが持つ分散情報及びメンバＩＤを（ｋ’，ｔ）しきい値秘密分散法を用いて分散し、他のメンバに配布する（ステップＳ１６０２）。ステップＳ１６０２は、図１３の秘密分散計算部１００１－ｊにおける動作を示しており、メンバＩＤがm’$_j$（ｊ＝１，２，…，ｔ）であるメンバの持つ分散情報Ｘm’$_j$を上記式（２９’）を用いて分散して、仮メンバＩＤがｄ$_p$（ｐ＝１，２，…，ｔ）であるメンバに対し、上記式（３０）で計算されるＸm’$_{j,p}$を配布し、メンバＩＤ＿m’$_j$を上記式（３１）を用いて分散して、仮メンバＩＤがｄ$_p$（ｐ＝１，２，…，ｔ）であるメンバに対し、上記式（３２）で計算されるm’$_{j,p}$を配布する。

【０１０８】

次に、各メンバは、公開されている集まったメンバの仮メンバＩＤ、自分自身の分散情報及びメンバＩＤのそれぞれの分散情報、及び、他のメンバから配布された分散情報及びメンバＩＤのそれぞれの分散情報を用いて演算を施し、もとの秘密情報Ｓの分散情報である値を求める（ステップＳ１６０３）。ステップＳ１６０３は、図１３の分散処理部１００２－ｊにおける動作を示しており、秘密再構成するための演算（上記式（３））を、メンバＩＤ＿m’$_j$（ｊ＝１，２，…，ｔ）及び分散情報Ｘm’$_j$を秘密にしたまま、上記式（３）の分散計算を行い、最終的に、仮メンバＩＤがｄ$_j$（ｊ＝１，２，…，ｔ）であるメンバは、再構成すればもとの秘密情報Ｓとなるような分散秘密情報Ｓｄ$_j$を得る。

【０１０９】

次に、ステップＳ１６０３で、各メンバが計算した分散情報及び仮メンバＩＤからもとの秘密情報Ｓを再構成する（ステップＳ１６０４）。ステップＳ１６０

４は、図１２の秘密再構成計算部９０３における動作を示しており、仮メンバＩＤがｄｊ（ｊ＝１，２，…，ｔ）であるメンバがステップＳ１６０３で計算した結果Ｓｄｊ（ｊ＝１，２，…，ｔ）、及び仮メンバＩＤ＿ｄｊ（ｊ＝１，２，…，ｔ）から、上記式（２７）を用いて計算し、もとの秘密情報Ｓを得ることができる。

【０１１０】

［第３の実施形態の効果］

以上説明したように、第３の実施形態によれば、上記第１及び第２の実施形態と同様に、もとの秘密情報Ｓを再構成するために集まったメンバの持つ分散情報を、他のメンバに公開せずに、もとの秘密情報Ｓを再構成することができる。したがって、各メンバが持つ分散情報を、次回の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを必要とせずに、上記の効果を達成することができる。

【０１１１】

また、第３の実施形態においては、第１の実施形態とは異なり、（ｋ，ｎ）しきい値秘密分散法を用いているので、必ずしもメンバ全員、すなわちｎ人が集まらなくとも、ｋ人（ｋ≦ｎ）以上が集まれば、もとの秘密情報Ｓを再構成することができる。

【０１１２】

さらに、第３の実施形態においては、第２の実施形態とは異なり、各メンバが保有する分散情報だけでなく、メンバＩＤをも公開せずに秘密情報の再構成を行なう。したがって、集まったメンバの匿名性を確保することができる。

【０１１３】

さらに、第３の実施形態においては、第１及び第２の実施形態と同様に、予め秘密情報Ｓの分散情報を持たない人（演算記憶装置）が、この再構成に参加しようとしても、もとの秘密情報Ｓの再構成に失敗することから、第３の実施形態においては、集まった複数人数からなるグループ全員が正当メンバ（予め秘密情報Ｓの分散情報を配布されたメンバ）か、そうでない人（演算記憶装置）が混在するか、ということを認証するような機能が、効果として備わる。さらに、前述の

ように再利用可能なので、この認証機能は、秘密情報Ｓの分散情報を更新せずとも何度も利用できる。また、この認証機能は、集まったメンバから他へ送信される情報は、認証（もとの秘密情報Ｓの再構成）のたびに異なるので、盗聴によるなりすましに非常に強い。特に、第３の実施形態においては、前述のように、「［１］もとの秘密情報Ｓの分散情報を持つメンバの全員が集まらなくとも、しきい値以上のメンバが集まればよい。［２］匿名性がある。」という２つの効果があることから、集まった複数人数からなるグループ全員が正当メンバであると認証された場合でも、どのメンバが集まっているかを具体的に特定せずに認証が可能である。このような認証機能は、秘密分散法の秘密再構成の性質と、マルチパーティ・プロトコルによる分散計算の性質との単なる組み合わせによって得られる機能ではなく、新しい機能である。ただし、第１、第２の実施形態の効果で説明したと同様に、上記認証機能は、「もとの秘密情報Ｓ」を照合秘密情報Ｓ（予め登録されている情報で、認証が成立するか否かを、再構成結果と照らし合わせる情報）として用いる利用形態であるので、もとの秘密情報Ｓを各メンバに秘密にしない場合であっても、実現できる。

【０１１４】

≪第４の実施形態≫

［第４の実施形態の概要］

上記第３の実施形態においては、もとの秘密情報Ｓを再構成する際に用いるマルチパーティ・プロトコルは、計算するために集まったメンバのうち、どの２人のメンバ間にも、その２人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されていることを前提とする方式（前述したマルチパーティ・プロトコルの第１方式）であったが、第４の実施形態においては、計算するために集まったメンバ間の通信には、上記秘密通信路を用いる通信手法に加え、紛失通信と呼ばれる通信手法を用いる方式（前述したマルチパーティ・プロトコルの第２方式）を用いる。これにより、第４の実施形態に係る秘密再構成方法によれば、第３の実施形態に係る秘密再構成方法による効果と同様の効果を得ることができる。さらに、第４の実施形態に係る秘密再構成方法によれば、上記第３の実施形態に係る秘密再構成方法における分散計算に用いる（ｋ’，ｔ）しきい値秘

密分散法のしきい値ｋ’の制限、すなわち、次式（２９）の制限、

ｋ’≦（ｔ＋１）／２　　…（２９）

を取り払い、しきい値ｋ’のとり得る範囲を、ｋ’≦ｔまで広げることができる。

【０１１５】

［第４の実施形態の構成］

第４の実施形態に係る秘密再構成方法を実施する構成（第４の実施形態に係る秘密再構成システム）は、上記第３の実施形態に係る秘密再構成方法を実施する構成とほぼ同じであるが、前述したマルチパーティ・プロトコルの第２方式を用いているので、図１６の“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成のみが異なる。第４の実施形態の説明においては、上記第３の実施形態に係る秘密再構成方法を実施する構成と異なる部分、すなわち、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成のみを説明する。

【０１１６】

図２０は、本発明の第４の実施形態に係る秘密再構成方法で使用される“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成を示すブロック図である。第４の実施形態においては、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａを、図２０に示されるように構成することによって、上記第３の実施形態における制限である、上記式（２９）の制限を取り払うことができる。このため、しきい値ｋ’のとり得る範囲を、ｋ’≦ｔまで広げることができる。図２０の構成は、前述したマルチパーティ・プロトコルの第２方式を利用している。

【０１１７】

次に、図２０を用いて、第４の実施形態における、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成を説明する。図２０に示されるように、第４の実施形態における“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａは、ｊｊ項計算部１７０１－ｊと、ｉｊ項計算部１７０２－ｊと、“（ｔ）加算部”１７０３－ｊとを有している。“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａに入力される２つの入力Ａｄｊ，Ｂｄｊは、ｊｊ項計算部１７０１－ｊと、ｉｊ項計算部１７０２－ｊとの両方に入力される。ｊｊ項計算部

１７０１－ｊからの出力及びｉｊ項計算部１７０２－ｊからの出力は、“（ｔ）加算部”１７０３－ｊに入力される。“（ｔ）加算部”１７０３－ｊからの出力が、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの出力となる。

【０１１８】

ｊｊ項計算部１７０１－ｊは、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａに入力される２つの入力Ａｄｊ，Ｂｄｊを受け取り、それらを乗算し、次式（４１）で計算される係数ｒｄｊをさらに乗算して、“（ｔ）加算部”１７０３－ｊに出力する。

【数２１】

$$rd_j=(d_1\times d_2\times\cdots\times d_t/d_j)$$
$$/((d_1-d_j)\times(d_2-d_j)\times\cdots\times(d_{j-1}-d_j)\times(d_{j+1}-d_j)\times\cdots\times(d_t-d_j))$$
$$=\prod_{\substack{i=1\\ i\neq j}}^{t} d_i/(d_i-d_j) \qquad (41)$$

【０１１９】

詳細に言えば、ｊｊ項計算部１７０１－ｊは、Ａｄｊ×Ｂｄｊを計算し、上記式（４１）の係数ｒｄｊをさらに掛けたｒｄｊ（Ａｄｊ×Ｂｄｊ）を計算して、出力する。

【０１２０】

ｉｊ項計算部１７０２－ｊは、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａに入力される２つの入力Ａｄｊ，Ｂｄｊを受け取り、受け取った入力Ａｄｊ，Ｂｄｊと秘密通信路３０３を通して他のメンバから受け取った情報から、実質的に他のメンバの値との乗算結果が得られるように計算をする。例えば、仮メンバＩＤがｄｊであるメンバは、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａに入力されるＡｄｊとＢｄｊの乗算Ａｄｊ×Ｂｄｊをｊｊ項計算部１７０１－ｊで行うが、ｉｊ項計算部１７０２－ｊにおいては、他のメンバ（メンバＩＤがｄｐであり、ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）の値との乗算、Ａｄｊ×Ｂｄｐ及びＡｄｐ×Ｂｄｊの結果に相当するもの（乗算結果そのものではない）が得られるようにする。

【０１２１】

ｉｊ項計算部１７０２－ｊは、

$Ad_j \times Bd_p = Dd_j + Dd_p$　　…（４２）

$Ad_p \times Bd_j = Ed_j + Ed_p$　　…（４２′）

となるような、Dd_j及びEd_jを仮メンバＩＤがd_jであるメンバが持つことができ、Dd_p及びEd_pを仮メンバＩＤがd_pであるメンバが持つことができるように、計算を行う。

【０１２２】

図２１は、図２０のｉｊ項計算部１７０２－ｊの構成を示すブロック図である。図２１を用いて、ｉｊ項計算部１７０２－ｊの構成を説明する。図２１に示されるように、ｉｊ項計算部１７０２－ｊは、ｊ－１個の項計算受信部１８０１－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）と、ｊ－１個の項計算受信部１８０２－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）と、ｔ－ｊ個の項計算送信部１８０３－ｊ－ｐ，（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）と、ｔ－ｊ個の項計算送信部１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）と、ｔ－１個の加算部１８０５－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）と、ｔ－１個の係数乗算部１８０６－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）とを有している。

【０１２３】

ｉｊ項計算部１７０２－ｊへ入力される２つの入力のうち、一つは、項計算受信部１８０１－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）及び項計算送信部１８０３－ｊ－ｐ（ｐ＝ｊ＋１、ｊ＋２，…，ｔ）へ、他の一つは、項計算受信部１８０２－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）及び項計算送信部１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）へ入力される。項計算受信部１８０１－ｊ－ｐ及び項計算受信部１８０２－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）からの出力は、加算部１８０５－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）へ入力され、項計算送信部１８０３－ｊ－ｐ及び項計算送信部１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）からの出力は、加算部１８０５－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）へ入力される。加算部１８０５－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）からの出力は係数乗算部１８０６－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）へ入力される。

【０１２４】

係数乗算部１８０６－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）からの出力（全部でｔ－１個の出力）が、ｉｊ項計算部１７０２－ｊからの出力となる。項計算受信部１８０１－ｊ－ｐ，１８０２－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）、及び項計算送信部１８０３－ｊ－ｐ，１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）は、秘密通信路３０３を通して、他のメンバとの情報のやりとりを行うことにより、前述の通り、他のメンバ（メンバＩＤがd_pであり、ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）の値との乗算、$Ad_j \times Bd_p$及び$Ad_p \times Bd_j$の結果に相当するもの（乗算結果そのものではない）が得られるようにするが、他のメンバの値Ad_p及びBd_p（メンバＩＤがd_pであり、ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）が分からないように、また、自分の値Ad_j及びBd_jが、他のメンバに分からないように、紛失通信を行う。紛失通信とは、ここでは、送信側が、Ｍ個の情報を符号化（暗号化）して送信するが、受信側においては、そのうち一つしか受け取る（意味のあるように復号が可能となる）ことができず、また、送信側においては、受信側がどの情報を受け取った（意味のあるように復号が可能となった）かを知ることができない通信方法をいう。この実施形態においては、法ｑのもとにおける離散対数を計算することが困難であることを利用して、紛失通信を構成する。

【０１２５】

項計算受信部１８０１－ｊ－ｐ，１８０２－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）、及び項計算送信部１８０３－ｊ－ｐ，１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）は、ｊの値によって、項計算受信部又は項計算送信部を持つ場合と、持たない場合とがある。例えば、ｊ＝１の場合には、項計算受信部を持たず、２×（ｔ－１）個の項計算送信部を持つ。また、ｊ＝ｔの場合には、項計算送信部を持たず、２×（ｔ－１）個の項計算受信部を持つ。また、他のメンバとの送受信の関係は、仮メンバＩＤがd_jであるメンバの項計算送信部１８０３－ｊ－ｐ，１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）からは、それぞれ、秘密通信路３０３を通して、仮メンバＩＤがd_pであるメンバの項計算受信部１８０１－ｐ－ｊ，１８０２－ｐ－ｊのそれぞれへ情報が渡される。これについては、

図２２及び図２３で説明する。

【０１２６】

加算部１８０５－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）は、項計算受信部１８０１－ｊ－ｐ，１８０２－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）、又は項計算送信部１８０３－ｊ－ｐ，１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）からの出力を受け取り、それらを加算して、係数乗算部１８０６－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ａ≠ｊであるもの）へ出力する。項計算受信部１８０１－ｊ－ｐ又は項計算送信部１８０３－ｊ－ｐからの出力を$Dd_{j,p}$とし、項計算受信部１８０２－ｊ－ｐ又は項計算送信部１８０４－ｊ－ｐからの出力を$Ed_{j,p}$とすると、加算部１８０５－ｊ－ｐにおいては、$Dd_{j,p}+Ed_{j,p}$を計算して、その計算結果を係数乗算部１８０６－ｊ－ｐへ出力する。

【０１２７】

係数乗算部１８０６－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）は、加算部１８０５－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）からの出力を受け取り、次式（４３）で計算される係数を乗算して出力する。

【数２２】

$$rd_p=(d_1\times d_2\times\cdots\times d_t/d_p)$$
$$/((d_1-d_p)\times(d_2-d_p)\times\cdots\times(d_{p-1}-d_p)\times(d_{p+1}-d_p)\times\cdots\times(d_t-d_p))$$
$$=\prod_{\substack{i=1\\ i\neq p}}^{t} d_i/(d_i-d_p) \qquad (43)$$

【０１２８】

加算部１８０５－ｊ－ｐからの出力を$Fd_{j,p}$とすると、係数乗算部１８０６－ｊ－ｐは、$rd_p\times Fd_{j,p}$を計算して、その計算結果を出力する。係数乗算部１８０６－ｊ－ｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）からの出力（全部でｔ－１個の出力）が、ｉｊ項計算部１７０２－ｊからの出力となる。

【０１２９】

次に、図２２を用いて、項計算受信部１８０１－ｊ－ｐ，１８０２－ｊ－ｐ（

ｐ＝１，２，…，ｊ－１）の構成を説明する。項計算受信部１８０１－ｊ－ｐ，１８０２－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）は、インデックス計算送信部１９０１－ｊ及び受信復元部１９０２－ｊからなる。項計算受信部１８０１－ｊ－ｐは、ｉｊ項計算部１７０２－ｊの２つの入力のうち一つの入力を受け取り、項計算受信部１８０２－ｊ－ｐは、他の一つの入力を受け取る。ここでは、項計算受信部１８０１－ｊ－ｐへの入力をＡｄｊ、項計算受信部１８０２－ｊ－ｐへの入力をＢｄｊとおく。項計算受信部１８０１－ｊ－ｐと１８０２－ｊ－ｐは、内部的に同じ構造なので、ここでは、項計算受信部１８０１－ｊ－ｐについて説明し、項計算受信部１８０２－ｊ－ｐに相当する説明は、括弧〔　〕の中に記述する。項計算受信部１８０１－ｊ－ｐ〔１８０２－ｊ－ｐ〕への入力は、インデックス計算送信部１９０１－ｊへ入力される。インデックス計算送信部１９０１－ｊからの出力は、受信復元部１９０２－ｊへ入力される。受信復元部１９０２－ｊからの出力が項計算受信部１８０１－ｊ－ｐ〔１８０２－ｊ－ｐ〕からの出力となる。

【０１３０】

インデックス計算送信部１９０１－ｊは、項計算受信部１８０１－ｊ－ｐ〔１８０２－ｊ－ｐ〕への入力Ａｄｊ〔Ｂｄｊ〕を受け取り、次式（４４）及び（４４′）で示す計算を施して、Ａ′ｄｊ，ｐ〔Ｂ′ｄｊ，ｐ〕を計算し、秘密通信路３０３を通して、仮メンバＩＤがｄｐであるメンバへ送信する（ｐ＝１，２，…，ｊ－１）。

【数２３】

$$A'd_{j,p} = g^{rAj,p}\, h^{Adj} \qquad (44)$$

$$B'd_{j,p} = g^{rBj,p}\, h^{Bdj} \qquad (44)'$$

【０１３１】

上記式（４４）及び（４４′）において、ｈ及びｇは、有限体ＧＦ（ｑ）上の２つの生成元とし、ｒＡｊ，ｐ〔ｒＢｊ，ｐ〕は、乱数として有限体ＧＦ（ｑ）上の値を選ぶ。また、インデックス計算送信部１９０１－ｊは、上記式（４４）〔（４４′）〕で用いた乱数ｒＡｊ，ｐ〔ｒＢｊ，ｐ〕を受信復元部１９０１

－ｊへ出力する。

【０１３２】

受信復元部１９０１－ｊは、仮メンバＩＤがｄｐ（ｐ＝１，２，…，ｊ－１）であるメンバからｑ個（ｑは有限体ＧＦ（ｑ）の要素数）の情報を受け取り、Ａｄｊ番目の情報Ｄ’ｄｊ，ｐ〔Ｂｄｊ番目の情報Ｅ’ｄｊ，ｐ〕を用いて、次式（４５）及び（４５’）で計算することにより、目的とする値Ｄｄｊ，ｐ〔Ｅｄｊ，ｐ〕を計算する（それ以外の受け取った情報は、仮メンバＩＤがｄｊであるメンバにとっては、乱数に見える）。Ｄ’ｄｊ，ｐ〔Ｅ’ｄｊ，ｐ〕は、２つの情報、Ｄ’１ｄｊ，ｐ及びＤ’２ｄｊ，ｐ〔Ｅ’１ｄｊ，ｐ及びＥ’２ｄｊ，ｐ〕から成っているものとする。

【数２４】

$$Dd_{j,p}=D'_1d_{j,p}/((D'_2d_{j,p})^{rAj,p}) \qquad (45)$$

$$Ed_{j,a}=E'_1d_{j,p}/((E'_2d_{j,p})^{rBj,p}) \qquad (45)'$$

上記式（４５）及び（４５’）で計算されるＤｄｊ，ｐ〔Ｅｄｊ，ｐ〕が、受信復元部１９０２－ｊの出力となり、項計算受信部１８０１－ｊ－ｐ〔１８０２－ｊ－ｐ〕からの出力となる。

【０１３３】

次に、図２３を用いて、項計算送信部１８０３－ｊ－ｐ，１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）の構成を説明する。図２３に示されるように、項計算送信部１８０３－ｊ－ｐ，１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）は、乱数生成部２００１－ｊと、有限体要素生成部２００２－ｊと、乗数計算送信部２００３－ｊ－ａ（ａ＝１，２，…，ｑ）とを有している。項計算送信部１８０３－ｊ－ｐ，１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）への入力は、乱数生成部２００１－ｊ及び有限体要素生成部２００２－ｊからの出力とともに、乗数計算送信部２００３－ｊ－ａ（ａ＝１，２，…，ｑ）へ入力される。乱数生成部２００１－ｊからの出力が、項計算送信部１８０３－ｊ－ｐ，１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）からの出力となる。項計算送信部１８０３－ｊ－ｐは、ｉｊ項計算部１７０２－ｊの２つの入力のうち一つの入力を

受け取り、項計算送信部１８０４－ｊ－ｐは、他の一つの入力を受け取る。ここでは、項計算送信部１８０３－ｊ－ｐへの入力をＡｄｊ、項計算送信部１８０４－ｊ－ｐへの入力をＢｄｊとおく。項計算送信部１８０３－ｊ－ｐと１８０４－ｊ－ｐは、内部的に同じ構造なので、ここでは、項計算送信部１８０３－ｊ－ｐについて説明し、項計算送信部１８０４－ｊ－ｐに相当する説明は、括弧〔　〕の中に記述する。

【０１３４】

乱数生成部２００１－ｊは、有限体ＧＦ（ｑ）上の値の乱数を生成して出力する。乗数計算送信部２００３－ｊ－ａ（ａ＝１，２，…，ｑ）へは、同じ乱数が出力される。乱数生成部２００１－ｊからの出力が項計算送信部１８０３－ｊ－ｐ〔１８０４－ｊ－ｐ〕（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）からの出力となる。

【０１３５】

有限体要素生成部２００２－ｊは、有限体ＧＦ（ｑ）上の値を０，１，…，ｑ－１と、順次生成し、それぞれ、乗数計算送信部２００３－ｊ－ａ（ａ＝１，２，…，ｑ）へ出力する。すなわち、乗数計算送信部２００３－ｊ－１へは０を、乗数計算送信部２００３－ｊ－２へは１を、乗数計算送信部２００３－ｊ－ｉへはｉ－１を、乗数計算送信部２００３－ｊ－ｑへはｑ－１を、出力する。

【０１３６】

乗数計算送信部２００３－ｊ－ａ（ａ＝１，２，…，ｑ）は、項計算送信部１８０３－ｊ－ｐ〔１８０４－ｊ－ｐ〕（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）から入力される値Ａｄｊ〔Ｂｄｊ〕、乱数生成部２００１－ｊからの乱数を、有限体要素生成部２００２－ｊから対応する有限体要素ａ－１を、秘密通信路３０３を通して仮メンバＩＤがｄｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）であるメンバからの情報（他のメンバの項計算受信部１８０１－ｐ－ｊ〔１８０２－ｐ－ｊ〕のインデックス計算送信部１９０１－ｐからの出力）Ａ’ｄｐ，ｊ〔Ｂ’ｄｐ，ｊ〕を、受け取り、それらの入力から計算をして、計算結果を出力する。乗数計算送信部２００３－ｊ－ａ（ａ＝１，２，…，ｑ）からの出力、合計ｑ個の出力は、秘密通信路３０３を通して、ａの小さい順に、仮メンバＩＤがｄｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）であるメンバへ送信する。

【０１３７】

今、乱数生成部２００１－ｊからの出力をＤｄｊ，ｐ〔Ｅｄｊ，ｐ〕とする。また、秘密通信路３０３を通して受信する値を、Ａ'ｄｐ，ｊ（項計算送信部１８０３－ｊ－ｐに相当）〔Ｂ'ｄｐ，ｊ（項計算送信部１８０４－ｊ－ｐに相当）〕とする。有限体要素生成部２００２－ｊから乗数計算送信部２００３－ｊ－ａ（ａ＝１，２，…，ｑ）へは、ａ－１が入力される。乗数計算送信部２００３－ｊ－ａ（ａ＝１，２，…，ｑ）は、次式（４６）、（４６′）、（４７）、（４７′）、（４８）、（４８′）の計算を行い、Ｄ'ｄｐ，ｊ，ａ〔Ｅ'ｄｐ，ｊ，ａ〕をそれぞれ計算し（Ｄ'ｄｐ，ｊ，ａ〔Ｅ'ｄｐ，ｊ，ａ〕は式（４５）〔式（４５′）〕の説明で述べたように２つの値からなる）、秘密通信路３０３を通して仮メンバＩＤがｄｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）であるメンバへ、ａ＝１，２，…，ｑの順に送信する。

【０１３８】

【数２５】

$$D'_1 d_{p,j,a} = g^{kA_a} \qquad (46)$$

$$E'_1 d_{p,j,a} = g^{kB_a} \qquad (46)'$$

$$D'_2 d_{p,j,a} = (A d_j (a-1) - D d_{j,p}) (A'd_{p,j} / h^a)^{kA_a} \qquad (47)$$

$$E'_2 d_{p,j,a} = (B d_j (a-1) - E d_{j,p}) (B'd_{p,j} / h^a)^{kB_a} \qquad (47)'$$

$$D'd_{p,j,a} = (D'_1 d_{p,j,a}, D'_2 d_{p,j,a}) \qquad (48)$$

$$E'd_{p,j,a} = (E'_1 d_{p,j,a}, E'_2 d_{p,j,a}) \qquad (48)'$$

【０１３９】

上記式において、ｋＡａ〔ｋＢａ〕（ａ＝１，２，…，ｑ）は、それぞれ、ｑ個の有限体ＧＦ（ｑ）上の値の乱数である。これらの出力Ｄ'ｄｐ，ｊ，ａ又はＥ'ｄｐ，ｊ，ａを秘密通信路３０３を通して、仮メンバＩＤがｄｐ（ｐ＝１＋１，ｊ＋２，…，ｔ）であるメンバの項計算受信部１８０１－ｐ－ｊ〔項計算受信部１８０２－ｐ－ｊ〕が受け取ると、受け取ったメンバは、ａ＝Ａｄｐ，ｊ〔Ｂｄｐ，ｊ〕に相当するａ番目の情報Ｄ'ｄｐ，ｊ＝Ｄ'ｄｐ，ｊ，ａ〔Ｅ'ｄｐ，ｊ＝Ｅ'ｄｐ，ｊ，ａ〕を式（４５）〔式（４５′）〕で復号することが

できる（それ以外の受け取った情報は、仮メンバＩＤがｄｐであるメンバにとっては、乱数に見える）。

【０１４０】

このように、図２０から図２３までに示されるような構成を採用した場合には、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａにおける式（２９）の制限をなくすことができる（すなわちｋ’≦ｔまで、しきい値ｋ’の範囲を拡大することができる）。

【０１４１】

[第４の実施形態の動作]

第４の実施形態に係る秘密再構成方法における動作は、上記第３の実施形態における動作とほぼ同じであり、図１９のフローチャートとほぼ同じであるが、図１９のステップＳ１６０３の動作に、異なる点を持つ。上記第３の実施形態においては、ステップＳ１６０３の計算に用いる“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａは、図１６のような構成で計算処理を行っていたが、第４の実施形態においては、図２０のような構成で計算処理を行う。

【０１４２】

[第４の実施形態の効果]

以上説明したように、第４の実施形態によれば、上記第１、第２、第３の実施形態と同様に、もとの秘密情報Ｓを再構成するために集まったメンバの持つ分散情報を、他のメンバに公開せずに、もとの秘密情報Ｓを再構成することができる。したがって、各メンバが持つ分散情報を、次回の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを必要とせずに、上記の効果を達成することができる。

【０１４３】

また、第４の実施形態においては、上記第３の実施形態と同様な効果を得ることができるだけでなく、上記第３の実施形態における、分散計算に用いる（ｋ’，ｔ）しきい値秘密分散法のしきい値ｋ’の制限、

ｋ’≦（ｔ＋１）／２　　…（２９）

を取り払い、ｋ’≦ｔまで、しきい値ｋ’のとり得る範囲を広げることができる。

【０１４４】

≪第５の実施形態≫

［第５の実施形態の概要］

上記第３の実施形態においては、図１５に示される分散逆元計算部１２０３－ｊ－ａ（ｊ＝１，２，…，ｔであり、ａ＝１，２，…，ｔである。）は、図１８に示されるように、（q_b－１）個の“（２）分散乗算部”を有している。これに対し、以下に説明する第５の実施形態によれば、分散逆元計算部１２０３－ｊ－ａ内に備えられる“（２）分散乗算部”の個数を減らすことができる。

【０１４５】

分散逆元計算部１２０３－ｊ－ａへ入力される値をA_jとし、この入力A_jと他のメンバの分散逆元計算部１２０３－ｐ－ａへ入力されるA_p（ｐ＝１，２，…，ｔであり、ｐ≠ｊである。）の、ｔ個の値A_p（ｐ＝１，２，…，ｔ）を分散情報として再構成されるようなもとの秘密情報をＡとすると、分散逆元計算部１２０３－ｊ－ａは、もとの秘密情報Ａの有限体ＧＦ（ｑ）上の逆元Ｃ＝Ａ$^{-1}$の、仮メンバＩＤがd_jであるメンバに対する分散情報C_jを計算する。第５の実施形態においては、分散逆元計算部１２０３－ｊ－ａへの入力値A_j（ｊ＝１，２，…，ｔ）に、各メンバそれぞれが生成した乱数B_j（ｊ＝１，２，…，ｔ）を用いて分散乗算することにより、入力値A_jを隠蔽した上で、その乱数B_jを分散乗算された値U_j（ｊ＝１，２，…，ｔ）を公開し、U_jを分散情報として再構成されるようなもとの秘密Ｕを再構成する。もとの秘密情報Ｕの逆元Ｕ$^{-1}$を算出し、逆元Ｕ$^{-1}$の分散情報$U^{-1}{}_j$を各メンバに分散する。各メンバは、その受け取った分散情報$U^{-1}{}_j$と発生させた乱数B_jから、求める値C_j＝$A^{-1}{}_j$を得る。

【０１４６】

［第５の実施形態の構成］

第５の実施形態の秘密再構成方法を実施する構成（第５の実施形態に係る秘密再構成システム）は、上記第３の実施形態に係る秘密再構成方法を実施する構成とほぼ同じであるが、図１５の分散逆元計算部１２０３－ｊ－ａ（ｊ＝１，２，…，ｔであり、ａ＝１，２，…，ｔである。）の構成のみが異なる。第５の実施

形態の説明においては、上記第３の実施形態と異なる部分、すなわち、分散逆元計算部１２０３－ｊ－ａの構成のみを説明する。

【０１４７】

図２４（ａ）及び（ｂ）を用いて、第５の実施形態の分散逆元計算部１２０３－ｊ－ａ（ｊ＝１，２，…，ｔであり、ａ＝１，２，…，ｔである。）の構成を説明する。図２４（ａ）は、集まったメンバのうち、ある代表メンバを一つ決定し（その仮メンバＩＤをd_jとする）、そのメンバの分散逆元計算部１２０３－ｊ－ａ（ａ＝１，２，…，ｔ）の構成を表している。この代表メンバは、どのように決定してもよいが、例えば、仮メンバＩＤが最小（又は最大）であるメンバにすると予め決めておくことで可能である。また、図２４（ｂ）は、その代表メンバ以外のメンバ（仮メンバＩＤをd_i（ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）とする）の分散逆元計算部１２０３－ｉ－ａ（ａ＝１，２，…，ｔ）の構成を表している。

【０１４８】

まず、代表メンバの分散逆元計算部１２０３－ｊ－ａ（図２４（ａ））を説明する。図２４（ａ）に示されるように、代表メンバの分散逆元計算部１２０３－ｊ－ａは、乱数生成部２１０１－ｊと、“（２）分散乗算部”２１０２－ｊと、２１０６－ｊと、線形結合計算部２１０３－ｊと、逆元計算部２１０４－ｊと、、秘密分散計算部２１０５－ｊとを有する。分散逆元計算部１２０３－ｊ－ａへの入力（Ａd_jとする）は、乱数生成部２１０１－ｊからの出力とともに、“（２）分散乗算部”２１０２－ｊへ入力される。“（２）分散乗算部”２１０２－ｊからの出力は、線形結合計算部２１０３－ｊへ入力され、線形結合計算部２１０３－ｊからの出力は、逆元計算部２１０４－ｊへ入力され、さらに、逆元計算部２１０４－ｊからの出力は、秘密分散計算部２１０５－ｊへ入力される。秘密分散計算部２１０５－ｊからの出力は、乱数生成部２１０１－ｊからの出力とともに“（２）分散乗算部”２１０６－ｊへ入力される。“（２）分散乗算部”２１０６－ｊからの出力が、代表メンバの分散逆元計算部１２０３－ｊ－ａからの出力となる。

【０１４９】

乱数生成部２１０１－ｊは、有限体ＧＦ（ｑ）上の値の乱数を生成して出力する。出力先は、“（２）分散乗算部”２１０２－ｊ及び２１０６－ｊで、両方に同じ乱数を出力する。

【０１５０】

“（２）分散乗算部”２１０２－ｊは、分散逆元計算部１２０３－ｊ－ａへの入力Ａｄ$_j$及び乱数生成部２１０１－ｊからの出力を受け取り、それらを入力として、秘密通信路３０３からの情報を用いながら演算を行い、その演算結果を、線形結合計算部２１０３－ｊへ出力する。第５の実施形態における“（２）分散乗算部”２１０２－ｊの構成は、図１６の“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成、又は、図２０の“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成と同じである。

【０１５１】

線形結合計算部２１０３－ｊは、“（２）分散乗算部”２１０２－ｊの出力結果、及び、秘密通信路３０３を通して他のメンバからの“（２）分散乗算部”２１０２－ｉ（後述する図２４（ｂ）、ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）の出力結果を受け取り、線形結合計算を行い、計算結果を逆元計算部２１０４－ｊへ出力する。第５の実施形態における線形結合計算部２１０３－ｊの構成は、図９の線形結合計算部７０２－ｊの構成と同様なものである。“（２）分散乗算部”２１０２－ｊの出力結果をＵｄ$_j$とし、秘密通信路３０３を通して他のメンバからの“（２）分散乗算部”２１０２－ｉ（後述する図２４（ｂ）、ｉ＝１，２，…，ｔでｉ≠ｊであるもの）の出力結果をＵｄ$_i$（ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）とすると、線形結合計算部２１０３－ｊは、前述した式（２５）及び（２６）と同様な次式（４９）及び（５０）を計算し、その結果Ｕを逆元計算部２１０４－ｊへ出力する。

【数２６】

$$U = rd_1 Ud_1 + rd_2 Ud_2 + \cdots + rd_t Ud_t = \sum_{p=1}^{t} rd_p Ud_p \quad (49)$$

$$rd_p = (d_1 \times d_2 \times \cdots \times d_t / d_p) / ((d_1 - d_p) \times (d_2 - d_p) \times \cdots \times (d_{p-1} - d_p) \times (d_{p+1} - d_p) \times \cdots \times (d_t - d_p)) = \prod_{i=1}^{t} d_i / (d_i - d_p) \quad (50)$$

【０１５２】

逆元計算部２１０４－ｊは、線形結合計算部２１０３－ｊからの出力Ｕを受け取り、その逆元Ｕ－１を計算して、秘密分散計算部２１０５－ｊへ出力する。有限体ＧＦ（ｑ）上の逆元は、もとの逆元をとりたい要素をｑ－２回乗算する次式（５１）、すなわち、

$U^{-1} = U^{q-2}$　…（５１）

で計算することもできる。また、ユークリッドの互除法を用いて計算することもできる。

【０１５３】

秘密分散計算部２１０５－ｊは、逆元計算部２１０４－ｊからの出力Ｕ－１を受け取り、この出力Ｕ－１を分散して、他のメンバに秘密通信路３０３を通して配布する。第５の実施形態における秘密分散計算部２１０５－ｊの構成は、図１６の秘密分散計算部１３０２－ｊの構成と同様なものである。第５の実施形態における秘密分散計算部２１０５－ｊは、次式（５２）のｋ’－１次多項式ｆ４（ｘ）を作る

【数２７】

$$f_4(x) = U^{-1} + R_{4,1} x + R_{4,2} x^2 + \cdots + R_{4,k'-1} x^{k'-1} \quad (52)$$

ここで、Ｒ４，１，Ｒ４，２，…，Ｒ４，ｋ’－１は、乱数として有限体ＧＦ（

ｑ）上の値をｋ’－１個選んだものである。

【０１５４】

秘密分散計算部２１０５－ｊは、仮メンバＩＤがｄｐ（ｐ＝１，２，…，ｔ）であるメンバに対して配布する分散情報Ｕ－１ｄｐを、上記式（５２）を用いて次式（５３）のように計算する。

【数２８】

$$U^{-1}d_p = f_4(d_p) = U^{-1} + R_{4,1}(d_p) + R_{4,2}(d_p)^2 + \cdots + R_{4,k'-1}(d_p)^{k'-1} \qquad (53)$$

【０１５５】

秘密分散計算部２１０５－ｊは、自分自身に対する分散情報Ｕ－１ｄｊは、“（２）分散乗算部”２１０６－ｊへ出力し、その他の分散情報Ｕ－１ｄｐ（ｐ＝１，２，…，ｔであり、ｐ≠ｊであるもの）を秘密通信路３０３を通して各メンバに配布する。

【０１５６】

“（２）分散乗算部”２１０６－ｊは、乱数生成部２１０１－ｊからの出力と、秘密分散計算部２１０５－ｊからの出力Ｕ－１ｄｊを受け取り、それらを入力として、秘密通信路３０３からの情報を用いながら演算を行い、その演算結果を出力する。第５の実施形態における“（２）分散乗算部”２１０６－ｊの構成は、図１６の“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成、又は、図２０の“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成と同じである。第５の実施形態においては、図２４（ａ）に示されるように、“（２）分散乗算部”２１０６－ｊからの出力が、仮メンバＩＤがｄｊである代表メンバの分散逆元計算部１２０３－ｊ－ａからの出力となる。

【０１５７】

次に、図２４（ｂ）を用いて、代表メンバ以外のメンバ（仮メンバＩＤをｄｉ（ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）とする）の分散逆元計算部１２０３－ｉ－ａ（ａ＝１，２，…，ｔ）の構成を説明する。図２４（ｂ）に示さ

れるように、代表メンバ以外のメンバの分散逆元計算部１２０３－ｉ－ａ（ａ＝１，２，…，ｔ）は、乱数生成部２１０１－ｉと、“（２）分散乗算部”２１０２－ｉ，２１０６－ｉと、公開送信部２１０７－ｉと、公開受信部２１０８－ｉとを有する。乱数生成部２１０１－ｉからの出力は、代表メンバ以外のメンバの分散逆元計算部１２０３－ｉ－ａへ入力される入力Ａｄ$_{i}$とともに、“（２）分散乗算部”２１０２－ｉへ入力される。また、乱数生成部２１０１－ｉからの出力は、“（２）分散乗算部”２１０６－ｉへも入力される。“（２）分散乗算部”２１０２－ｉからの出力は、公開送信部２１０７－ｉへ入力される。乱数生成部２１０１－ｉからの出力は、公開受信部２１０８－ｉからの出力とともに、“（２）分散乗算部”２１０６－ｉへ入力される。“（２）分散乗算部”２１０６－ｉからの出力が、代表メンバ以外のメンバの分散逆元計算部１２０３－ｉ－ａからの出力となる。

【０１５８】

図２４（ｂ）の乱数生成部２１０１－ｉの構成及び動作は、図２４（ａ）の乱数生成部２１０１－ｊの構成及び動作と同様である。また、図２４（ｂ）の“（２）分散乗算部”２１０２－ｉ，２１０６－ｉの構成及び動作は、図２４（ａ）の“（２）分散乗算部”２１０２－ｊ，２１０６－ｊの構成及び動作と同様である。

【０１５９】

公開送信部２１０７－ｉは、“（２）分散乗算部”２１０２－ｉからの出力を受け取り、それを、秘密通信路３０３を通して、代表メンバへ送信する。“（２）分散乗算部”２１０２－ｉからの出力をＵｄ$_{i}$とすると、代表メンバ以外の公開送信部２１０７－ｉ（ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）からの出力Ｕｄ$_{i}$を、秘密通信路３０３を通して、代表メンバの線形結合計算部２１０３－ｊへ送信し、代表メンバの線形結合計算部２１０３－ｊは合計でｔ－１個のＵｄ$_{i}$（ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）を受け取る。

【０１６０】

公開受信部２１０８－ｉは、秘密通信路３０３を通して、代表メンバの秘密分散計算部２１０５－ｊからＵ$^{-1}$ｄ$_{i}$を受け取り、それを“（２）分散乗算部”

２１０６－ｉへ入力する。

【０１６１】

“（２）分散乗算部”２１０６－ｉは、乱数生成部２１０１－ｉからの出力、及び、公開受信部２１０８－ｉからの出力を受け取り、それらを入力として、秘密通信路３０３からの情報を用いながら演算を行い、その演算結果を出力する。第５の実施形態における“（２）分散乗算部”２１０６－ｉの構成は、図１６の“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成、又は、図２０の“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａの構成と同じである。図２４（ｂ）に示されるように、“（２）分散乗算部”２１０６－ｉからの出力が、代表メンバ以外のメンバの分散逆元計算部１２０３－ｉ－ａからの出力となる。

【０１６２】

このように、図２４の構成をとると、分散逆元計算部１２０３－ｉ－ａの“（２）分散乗算部”の個数を減らすことができ、処理を簡素化することができる。

【０１６３】

[第５の実施形態の動作]

第５の実施形態に係る秘密再構成方法における動作は、上記第３の実施形態における動作とほぼ同じであり、図１９のフローチャートとほぼ同じであるが、図１９のステップＳ１６０３の動作が、異なる点を持つ。上記第３の実施形態においては、ステップＳ１６０３の計算に用いる分散逆元計算部１２０３－ｉ－ａは、図１８のような構成により計算処理を行っていたが、第５の実施形態においては、図２４のような構成により計算処理を行う。

【０１６４】

[第５の実施形態の効果]

以上説明したように、第５の実施形態によれば、上記第１、第２、第３の実施形態と同様に、もとの秘密情報Ｓを再構成するために集まったメンバの持つ分散情報を、他のメンバに公開せずに、もとの秘密情報Ｓを再構成することができる。したがって、各メンバが持つ分散情報を、次回の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを必

要とせずに、上記の効果を達成することができる。

【０１６５】

また、第５の実施形態においては、上記第３の実施形態と同様な効果を得ることができるだけでなく、上記第３の実施形態における、分散逆元計算部１２０３－ｊ－ａ（ｊ＝１，２，…，ｔ、ａ＝１，２，…，ｔ）の“（２）分散乗算部”の個数を格段に減らすことができる。

【０１６６】

≪変形例≫

［第１の実施形態の変形例］

上記第１の実施形態においては、メンバのうち、どの２人のメンバ間にも、その２人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されていることを前提としていたが、マルチパーティ・プロトコルで用いる秘密分散法に、加算秘密分散法を用いているため、すべてを盗聴されていたとしても秘密再構成は不可能であり、秘密通信路ではなく、秘密通信路ではない（盗聴される可能性のある）通信路で通信してもよい。

【０１６７】

［第３の実施形態の変形例］

図２５は、本発明の第３の実施形態の変形例における項計算部１１０１－ｊ－ａの構成を示すブロック図である。上記第３の実施形態における項計算部１１０１－ｊ－ａにおいては、図１５（第３の実施形態）に示されるように、“（２）分散乗算部”１２０５－ｊ－ａ及び“（２）分散乗算部”１２０６－ｊ－ａは、項計算部１１０１－ｊ－ａへ入力されるＸｍ’ａ，ｊと、分散逆元計算部１２０３－ｊ－ａからの出力と、“（ｔ－１）分散乗算部”１２０４－ｊ－ａからの出力とを分散計算により掛け合わす処理を行っていたが、図１５に示される“（２）分散乗算部”１２０５－ｊ－ａ及び“（２）分散乗算部”１２０６－ｊ－ａを、図２５に示されるように、１つの“（３）分散乗算部”１２０７－ｊ－ａに置き換えることも可能である。図２５に示されるように、“（３）分散乗算部”１２０７－ｊ－ａは、入力される３つの値の分散乗算を行う部分であり、“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａと同様な構成（すなわち

、ｔ－１＝３とした構成）で実施できる。

【０１６８】

また、上記第３の実施形態においては、図１７（第３の実施形態）に示されるように、“（ｔ－１）分散乗算部”１２０２－ｊ－ａ，１２０４－ｊ－ａは、入力される値を、Ａ１，Ａ２，…，Ａ（ｔ－１）と、Ａのインデックス（下付き添え字）が小さい順に分散乗算するように構成している。しかし、分散乗算の順序は入れ替え可能なので、必ずしもこの順番（Ａのインデックス（下付き添え字）が小さい順）に分散乗算するように構成する必要はない。

【０１６９】

［第２の実施形態の変形例］

上記第２の実施形態においては、分散秘密再構成計算部６０１－ｊの秘密分散計算部７０１－ｊ、及び、秘密再構成計算部６０２が、それぞれ、（ｋ’、ｔ）しきい値秘密分散法による、秘密分散、及び、秘密再構成を行っている場合を説明したが、これに代えて、加算秘密分散法による、秘密分散、及び、秘密再構成を行うように構成してもよい。その場合には、秘密再構成計算部６０２において計算する上記式（２２）及び（４）に代えて、次式（５４）のような計算処理を行う。

【数２９】

$$S = Sm'_1 + Sm'_2 + \cdots + Sm'_t = \sum_{j=1}^{t} Sm'_j \qquad (54)$$

また、秘密分散計算部７０１－ｊにおいて計算する上記式（２３）及び（２４）に代えて、次のような計算により分散情報Ｘｍ’ｊ，ｐを求める。まず、乱数として有限体ＧＦ（ｑ）の値をｔ－１個選んで、分散情報Ｘｍ’ｊ，ｐ（ｐ＝１、２、…、ｔ－１）に割り当て、Ｘｍ’ｊ，ｔを次式（５５）のように求める。

Ｘｍ’ｊ，ｔ

＝Ｘｍ’ｊ－（Ｘｍ’ｊ，１＋Ｘｍ’ｊ，２＋…＋Ｘｍ’ｊ，ｔ－１）　　（５５）

【０１７０】

［第４の実施形態の変形例］

図２６は、本発明の第４の実施形態の変形例におけるｉｊ項計算部１７０２－ｊの構成を示すブロック図である。上記第４の実施形態においては、第３の実施形態に係る秘密再構成方法における分散計算に用いる（ｋ’，ｔ）しきい値秘密分散法のしきい値ｋ’の式（２９）の制限を取り払うことができるので、（ｋ’，ｔ）しきい値秘密分散法の代わりに、加算秘密分散法を用いることができる。分散秘密再構成計算部９０２－ｊの秘密分散計算部１００１－ｊにおける計算処理、秘密再構成計算部９０３における計算処理、及び、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａにおけるｊｊ項計算部１７０１－ｊにおける計算処理とｉｊ項計算部１７０２－ｊにおける構成を変更することにより、分散計算に用いる秘密分散法を加算秘密分散計算法に変更することができる。まず、分散秘密再構成計算部９０２－ｊの秘密分散計算部１００１－ｊにおける計算処理は、式（２９′）及び（３０）を用いて分散情報Ｘｍ’ｊ，ｐを求める代わりに、次のような計算処理に変更する。まず、乱数として有限体ＧＦ（ｑ）の値をｔ－１個選んで、Ｘｍ’ｊ，ｐ（ｐ＝１，２，…，ｔ－１）に割り当て、Ｘｍ’ｊ，ｔを次式（５６）のように求める。

Ｘｍ’ｊ，ｔ
＝Ｘｍ’ｊ－（Ｘｍ’ｊ，１＋Ｘｍ’ｊ，２＋…＋Ｘｍ’ｊ，ｔ－１）　　（５６）

また、秘密再構成計算部９０３における計算処理は、式（２７）及び（２８）を用いる代わりに、次式（５７）のような計算処理に変更する。

【数３０】

$$S = Sd_1 + Sd_2 + \cdots + Sd_t = \sum_{j=1}^{t} Sd_j \qquad (57)$$

さらに、上記第４の実施形態においては、図２１（第４の実施形態）に示されるように、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａにおけるｊｊ項計算部１７０１－ｊにおける計算処理は、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａに入力される２つの入力Ａｄｊ，Ｂｄｊを受け取りそ

れらを乗算して、式（４１）で計算される係数ｒｄｊをさらに乗算する。しかし、第４の実施形態の変形例においては、図２６に示されるように、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａは、係数ｒｄｊの乗算を省略するように構成されている。すなわち、第４の実施形態の変形例においては、Ａｄｊ×Ｂｄｊを計算して出力するようにするため、図２１（第４の実施形態）に示される係数乗算部１８０６－ｊ－ｉ（ｉ＝１，２，…，ｊ－１，ｊ＋１，…，ｔ）の構成部分が削除されている。

【０１７１】

［第５の実施形態の変形例］

図２７（ａ）及び（ｂ）は、本発明の第５の実施形態の変形例における分散逆元計算部１２０３－ｊ－ａ，１２０３－ｉ―ａの構成を示すブロック図である。上記第５の実施形態においては、第３の実施形態に係る秘密再構成方法における分散計算に用いる（ｋ’，ｔ）しきい値秘密分散法のしきい値ｋ’の式（２９）の制限を取り払うことができる場合も考慮でき、その場合には、（ｋ’，ｔ）しきい値秘密分散法の代わりに、加算秘密分散法を用いることができる。上記の第４の実施形態の変更（すなわち、分散秘密再構成計算部９０２－ｊの秘密分散計算部１００１－ｊにおける計算処理、秘密再構成計算部９０３における計算処理、及び、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａにおけるｊｊ項計算部１７０１－ｊにおける計算処理とｉｊ項計算部１７０２－ｊにおける構成を変更する）に加え、さらに、分散逆元計算部１２０３－ｊ－ａ，１２０３－ｉ－ａを図２４（第５の実施形態）の構成から図２７（第５の実施形態の変形例）のような構成に変更することにより、分散計算に用いる秘密分散法を加算秘密分散計算法に変更することができる。線形結合計算部２１０３－ｊを、“（ｔ）加算部”２１０９－ｊに変更し、秘密分散計算部２１０５－ｊ内の計算処理を変更する。秘密分散計算部２１０５－ｊの処理を変更するので、図２７では、符号２１１０－ｊを付与する。“（ｔ）加算部”２１０９－ｊは、“（２）分散乗算部”２１０２－ｊの出力結果、及び、秘密通信路３０３を通して他のメンバからの“（２）分散乗算部”２１０２－ｉ（ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）の出力結果を受け取り、それらをすべて加算して、計算結果を逆元計算

部２１０４－ｊへ出力する。“（２）分散乗算部”２１０２－ｊの出力結果をＵｄｊとし、秘密通信路３０３を通して他のメンバからの“（２）分散乗算部”２１０２－ｉ（ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）の出力結果をＵｄｉ（ｉ＝１，２，…，ｔであり、ｉ≠ｊであるもの）とすると、線形結合計算部２１０３－ｊでは、式（４９）および（５０）の計算処理を行って、その結果のＵを出力していたが、“（ｔ）加算部”２１０９－ｊは、次式（５８）を計算し、その結果Ｕを逆元計算部２１０４－ｊへ出力する。

【数３１】

$$U=Ud_1+Ud_2+\cdots+Ud_t=\sum_{p=1}^{t}Ud_p \qquad (58)$$

また、秘密分散計算部２１０５－ｊの処理を変更した秘密分散計算部２１１０－ｊは、逆元計算部２１０４－ｊからの出力Ｕ$^{-1}$を受け取り、この出力Ｕ$^{-1}$を分散して他のメンバに秘密通信路３０３を通して配布する。秘密分散計算部２１０５－ｊは、式（５２）及び（５３）の計算処理を行って分散情報Ｕ$^{-1}$ｄｐ（ｐ＝１，２，…，ｔ）を求めていたが、秘密分散計算部２１１０－ｊは、次のように分散情報Ｕ$^{-1}$ｄｐ（ｐ＝１，２，…，ｔ）を求める。まず、乱数として有限体ＧＦ（ｑ）の値をｔ－１個選んで、Ｕ$^{-1}$ｄｐ（ｐ＝１，２，…，ｔ－１）に割り当て、Ｕ$^{-1}$ｄｔを次式のように求める。

$$U^{-1}d_t=U^{-1}-(U^{-1}d_1+U^{-1}d_2+\cdots+U^{-1}d_{t-1}) \qquad (59)$$

【０１７２】

［他の変形例］

上記第４の実施形態（及び上記第４の実施形態の変形例）における、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａにおいて、①項計算受信部１８０１－ｊ－ｐ（ｐ＝１，２，…，ｊ－１）を項計算送信部に置き換え、さらに、項計算送信部１８０３－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）を項計算受信部に置き換えた構成、又は、②項計算受信部１８０２－ｊ－ｐ（ｐ＝１，２，…

，ｊ－１）を項計算送信部に置き換え、さらに、項計算送信部１８０４－ｊ－ｐ（ｐ＝ｊ＋１，ｊ＋２，…，ｔ）を項計算受信部に置き換えた構成、又は、③項計算受信部をすべて項計算送信部に、さらに、項計算送信部をすべて項計算受信部に置き換えた構成、などの構成でも、同様の効果を得ることができる。

【０１７３】

また、上記第４の実施形態（及び上記第４の実施形態の変形例）における、“（２）分散乗算部”１２０５－ｊ－ａ，１２０６－ｊ－ａにおいて、項計算送信部１８０１－ｊ－ｐ（又は１８０２－ｊ－ｐ）と項計算受信部１８０３－ｐ－ｊ（又は１８０４－ｐ－ｊ）との間の秘密通信路３０３における情報のやり取りは、式（４４）（又は式（４４′））や式（４６）～（４８）（又は式（４６′）～（４８′））のように、暗号化されたような情報、すなわち、法ｑのもとにおける離散対数を計算することが困難であること利用して送りたい情報を隠蔽している情報なので、とくに秘密に通信する必要はない。式（４４）（又は式（４４′））においては、送りたい情報Ａｄｊ（又はＢｄｊ）を有限体ＧＦ（ｑ）の生成元ｈのべき数として隠蔽し、式（４６）～（４８）（又は式（４６′）～（４８′））で得られる情報から得るべき必要な情報Ａｄｊ（ａ－１）－Ｄｄｊ，ｐ（又はＢｄｊ（ａ－１）－Ｅｄｊ，ｐ）は、式（４４）（又は式（４４′））で用いた乱数ｒＡｐ，ｊ（又はｒＢｐ，ｊ）を知らないと算出できないようになっている。したがって、上記における通信においては、秘密通信路ではない通信路（すなわち、放送型の通信路や盗聴される可能性のある通信路）で通信してもよい。

【０１７４】

また、上記第５の実施形態（及び上記第５の実施形態の変形例）における、分散逆元計算部１２０３－ｊ－ａにおいて、代表メンバの分散逆元計算部１２０３－ｊ－ａにおける線形結合計算部２１０３－ｊ（及び“（ｔ）加算部”２１０９－ｊ）、逆元計算部２１０４－ｊ、及び秘密分散計算部２１０５－ｊ（２１１０－ｊ）の処理（各メンバから“（２）分散乗算部”２１０２－ｉからの出力を集めて線形結合計算（加算）を行い、その結果の逆元を求め、求めた逆元をさらに秘密分散して各メンバに配布する処理）は、統合するセンターのようなものが行

い、代表メンバなしで実施する、すなわち、集まったメンバすべての分散逆元計算部２１０３－ｊ－ａが、図２４（ｂ）のような構成をとることもできる。

【０１７５】

また、上記第５の実施形態（及び上記第５の実施形態の変形例）における、分散逆元計算部１２０３－ｊ－ａにおいて、代表メンバの線形結合計算部２１０３－ｊ（及び“（ｔ）加算部”２１０９－ｊ）、と秘密通信路３０３との情報のやり取り（すなわち、代表メンバ以外のメンバの公開送信部２１０７－ｉと秘密通信路３０３との情報のやり取り）、及び、代表メンバの秘密分散計算部２１０５－ｊと秘密通信路３０３との情報のやり取り（すなわち、代表メンバ以外のメンバの公開受信部２１０８－ｉと秘密通信路３０３との情報のやり取り）は、とくに秘密に通信する必要はないので、放送型の通信路や盗聴される可能性のある通信路で通信してもよい。

【０１７６】

また、上記第１～第５の実施形態においては「メンバ」を、演算記憶装置であるとして説明したが、本発明に係る秘密再構成方法は、複数のメンバ（人間）が分散情報を持ち寄って、複数の人間が秘密再構成処理を進めることもできる。

【０１７７】

さらに、上記第１～第５の実施形態において、上記第１～第３の実施形態の説明の効果として記述したように、集まった複数人からなるグループ全員が正当メンバ（予め秘密情報Ｓの分散情報を配布されたメンバ）か、そうでない人（装置）が混在するか、ということを認証するような機能があるので、その場合には、「もとの秘密情報Ｓ」は、照合秘密情報Ｓ（予め登録されている情報で、認証が成立するか否かを、再構成結果と照らし合わせる情報）として用いるため、必ずしもメンバに秘密な情報でなくても実現できる。

【０１７８】

【発明の効果】

以上説明したように、本発明によれば、各メンバが保有する分散情報又はメンバＩＤを公開せずに、もとの秘密情報の再構成を行うことができるという効果が得られる。

【図面の簡単な説明】

【図１】　（ｋ，ｎ）しきい値秘密分散法を実施する構成を示す図である。

【図２】　本発明の第１の実施形態における秘密分散法を実施する構成を示す図である。

【図３】　本発明の第１の実施形態における各メンバ及び秘密通信路を示す図である。

【図４】　本発明の第１の実施形態に係る秘密再構成方法の概要を説明するための図である。

【図５】　本発明の第１の実施形態に係る秘密再構成方法を実施する構成（秘密再構成システム）を示すブロック図である。

【図６】　図５の分散秘密再構成計算部（分散秘密再構成装置）の構成を示すブロック図である。

【図７】　本発明の第１の実施形態に係る秘密再構成方法における動作を示すフローチャートである。

【図８】　本発明の第２の実施形態に係る秘密再構成方法を実施する構成（秘密再構成システム）を示すブロック図である。

【図９】　図８の分散秘密再構成計算部（分散秘密再構成装置）の構成を示すブロック図である。

【図１０】　本発明の第２の実施形態に係る秘密再構成方法における動作を示すフローチャートである。

【図１１】　本発明の第３の実施形態に係る秘密再構成方法の概要を説明するための図である。

【図１２】　本発明の第３の実施形態に係る秘密再構成方法を実施する構成（秘密再構成システム）を示すブロック図である。

【図１３】　図１２の分散秘密再構成計算部（分散秘密再構成装置）の構成を示すブロック図である。

【図１４】　図１３の分散処理部の構成を示すブロック図である。

【図１５】　図１４の項計算部の構成を示すブロック図である。

【図１６】　図１５の“（２）分散乗算部”の構成を示すブロック図である

。

【図１７】　図１５の“（ｔ－１）分散乗算部”の構成を示すブロック図である。

【図１８】　図１５の分散逆元計算部の構成を示すブロック図である。

【図１９】　本発明の第３の実施形態に係る秘密再構成方法における動作を示すフローチャートである。

【図２０】　本発明の第４の実施形態に係る秘密再構成方法で使用される“（２）分散乗算部”の構成を示すブロック図である。

【図２１】　図２０のｉｊ項計算部の構成を示すブロック図である。

【図２２】　図２１の項計算受信部の構成を示すブロック図である。

【図２３】　図２１の項計算送信部の構成を示すブロック図である。

【図２４】　本発明の第５の実施形態に係る秘密再構成方法で使用される分散逆元計算部の構成を示すブロック図である。

【図２５】　本発明の第３の実施形態の変形例における項計算部の構成を示すブロック図である。

【図２６】　本発明の第４の実施形態の変形例におけるｉｊ項計算部の構成を示すブロック図である。

【図２７】　本発明の第５の実施形態の変形例における分散逆元計算部の構成を示すブロック図である。

【符号の説明】

２０１　秘密分散計算部、

３０１　メンバの分散秘密再構成計算部（分散秘密再構成装置）、

３０１－ｊ　メンバｊの分散秘密再構成計算部、

３０２　秘密再構成装置の秘密再構成計算部、

３０３　秘密通信路、

４０１－ｊ　メンバｊのの秘密分散計算部、

４０２－ｊ　メンバｊの“（ｎ）加算部”、

６０１　メンバの分散秘密再構成計算部（分散秘密再構成装置）、

６０１－ｊ　メンバＩＤがm_jであるメンバの分散秘密再構成計算部、

６０２　秘密再構成装置の秘密再構成計算部、

７０１－ｊ　メンバＩＤがm_jであるメンバの秘密分散計算部、

７０２－ｊ　メンバＩＤがm_jであるメンバの線形結合計算部、

９０１　仮メンバＩＤ生成部、

９０２　メンバの分散秘密再構成計算部（分散秘密再構成装置）、

９０２－ｊ　仮メンバＩＤがd_jであるメンバの分散秘密再構成計算部、

９０３　秘密再構成装置の秘密再構成計算部、

１００１－ｊ　仮メンバＩＤがd_jであるメンバの秘密分散計算部、

１００２－ｊ　仮メンバＩＤがd_jであるメンバの分散処理部、

１１０１－ｊ－ａ（ａ＝１，２，…，ｔ）　仮メンバＩＤがd_jであるメンバの項計算部、

１１０２－ｊ　仮メンバＩＤがd_jであるメンバの“（ｔ）加算部”、

１２０１－ｊ－ａ（ａ＝１，２，…，ｔ）　仮メンバＩＤがd_jであるメンバの差分計算部、

１２０２－ｊ－ａ（ａ＝１，２，…，ｔ）　仮メンバＩＤがd_jであるメンバの“（ｔ－１）分散乗算部”、

１２０３－ｊ－ａ（ａ＝１，２，…，ｔ）　仮メンバＩＤがd_jであるメンバの分散逆元計算部、

１２０４－ｊ－ａ（ａ＝１，２，…，ｔ）　仮メンバＩＤがd_jであるメンバの“（ｔ－１）分散乗算部”、

１２０５－ｊ－ａ（ａ＝１，２，…，ｔ）　仮メンバＩＤがd_jであるメンバの“（２）分散乗算部”、

１２０６－ｊ－ａ（ａ＝１，２，…，ｔ）　仮メンバＩＤがd_jであるメンバの“（２）分散乗算部”、

１３０１－ｊ　仮メンバＩＤがd_jであるメンバの乗算部、

１３０２－ｊ　仮メンバＩＤがd_jであるメンバの秘密分散計算部、

１３０３－ｊ　仮メンバＩＤがd_jであるメンバの線形結合計算部、

１４０１－１，…，１４０１－（ｔ－２）　“（２）分散乗算部”、

１５０１－１，…，１５０１－（q_b－１）　“（２）分散乗算部”、

１５０２　乗算制御部、

１５０３　（ｑｂ）分散乗算部、

１７０１－ｊ　仮メンバＩＤがｄｊであるメンバのｊｊ項計算部、

１７０２－ｊ　仮メンバＩＤがｄｊであるメンバのｉｊ項計算部、

１７０３－ｊ　仮メンバＩＤがｄｊであるメンバの“（ｔ）加算部”、

１８０１－ｊ－１，…，１８０１－ｊ－（ｊ－１）　仮メンバＩＤがｄｊであるメンバの項計算受信部、

１８０２－ｊ－１，…，１８０２－ｊ－（ｊ－１）　仮メンバＩＤがｄｊであるメンバの項計算受信部、

１８０３－ｊ－（ｊ＋１），…，１８０３－ｊ－ｔ　仮メンバＩＤがｄｊであるメンバの項計算送信部、

１８０４－ｊ－（ｊ＋１），…，１８０４－ｊ－ｔ　仮メンバＩＤがｄｊであるメンバの項計算送信部、

１８０５－ｊ－１，…，１８０５－ｊ－（ｊ－１），１８０５－ｊ－（ｊ＋１），…，１８０５－ｊ－ｔ　仮メンバＩＤがｄｊであるメンバの加算部、

１８０６－ｊ－１，…，１８０６－ｊ－（ｊ－１），１８０６－ｊ－（ｊ＋１），…，１８０６－ｊ－ｔ　仮メンバＩＤがｄｊであるメンバの係数乗算部、

１９０１－ｊ　仮メンバＩＤがｄｊであるメンバのインデックス計算送信部、

１９０２－ｊ　仮メンバＩＤがｄｊであるメンバの受信復元部、

２００１－ｊ　仮メンバＩＤがｄｊであるメンバの乱数生成部、

２００２－ｊ　仮メンバＩＤがｄｊであるメンバの有限体要素生成部、

２００３－ｊ－１，…，２００３－ｊ－ｑ　仮メンバＩＤがｄｊであるメンバの乗算計算送信部、

２１０１－ｊ　仮メンバＩＤがｄｊであるメンバの乱数生成部、

２１０２－ｊ　仮メンバＩＤがｄｊであるメンバの“（２）分散乗算部”、

２１０３－ｊ　仮メンバＩＤがｄｊであるメンバの線形結合計算部、

２１０４－ｊ　仮メンバＩＤがｄｊであるメンバの逆元計算部、

２１０５－ｊ　仮メンバＩＤがｄｊであるメンバの秘密分散計算部、

２１０６－ｊ　仮メンバＩＤがｄｊであるメンバの“（２）分散乗算部”、

２１０７－ｉ　仮メンバＩＤがd_jであるメンバの公開送信部、

２１０８－ｉ　仮メンバＩＤがd_jであるメンバの公開受信部、

Ｓ　もとの秘密情報、

m_1，m_2，…，m_n　メンバＩＤ、

m'_1，m'_2，…，m'_t　集まったメンバのメンバＩＤ、

d_1，d_2，…，d_t　仮メンバＩＤ、

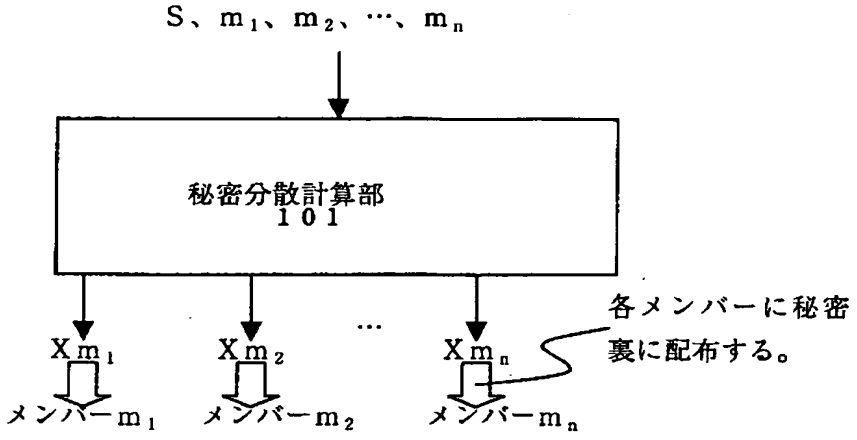
Xm_j　メンバＩＤがm_jであるメンバに配布される分散情報、

$Xm_{j,p}$　メンバＩＤがm_jであるメンバからメンバＩＤがm_pであるメンバｐに対して配布する分散情報、

S_j　メンバｊが分散再構成した分散情報。

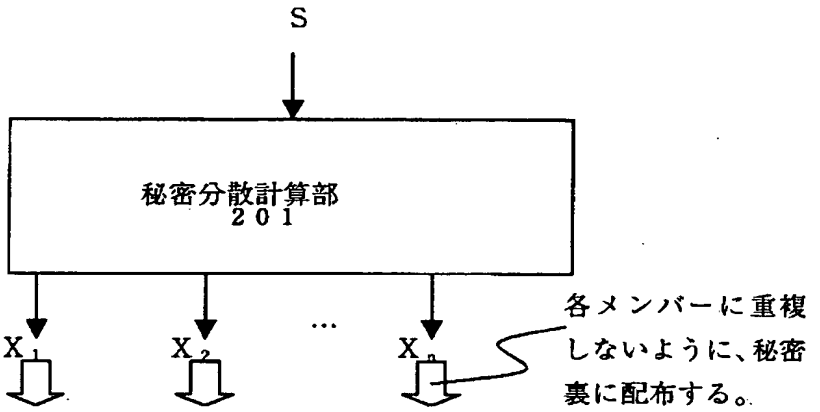
【書類名】　図面

【図１】



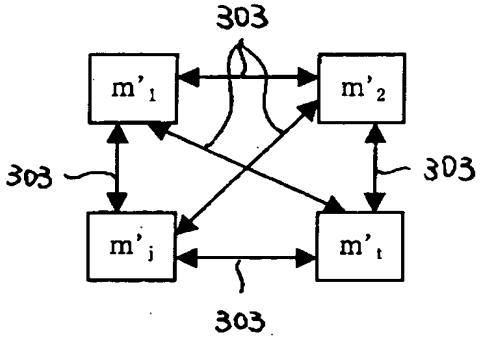
(k，n)しきい値秘密分散法

【図２】



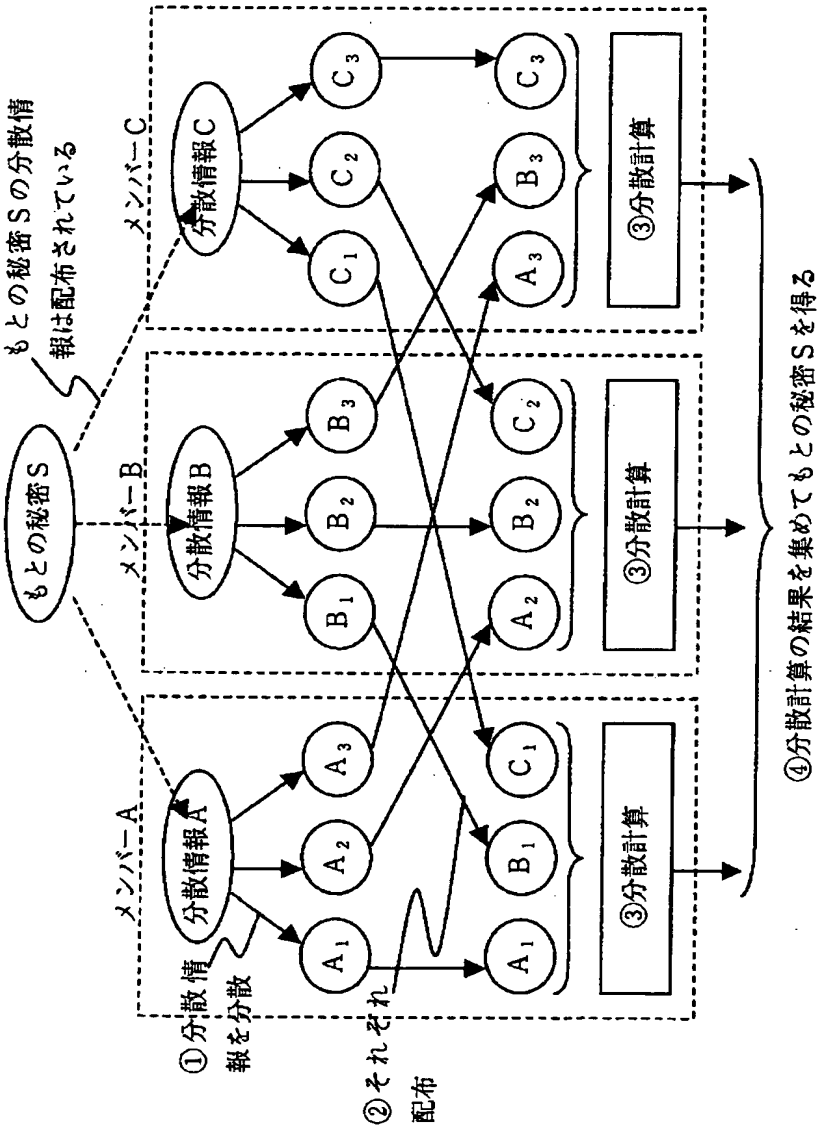
第１の実施形態における秘密分散

【図３】



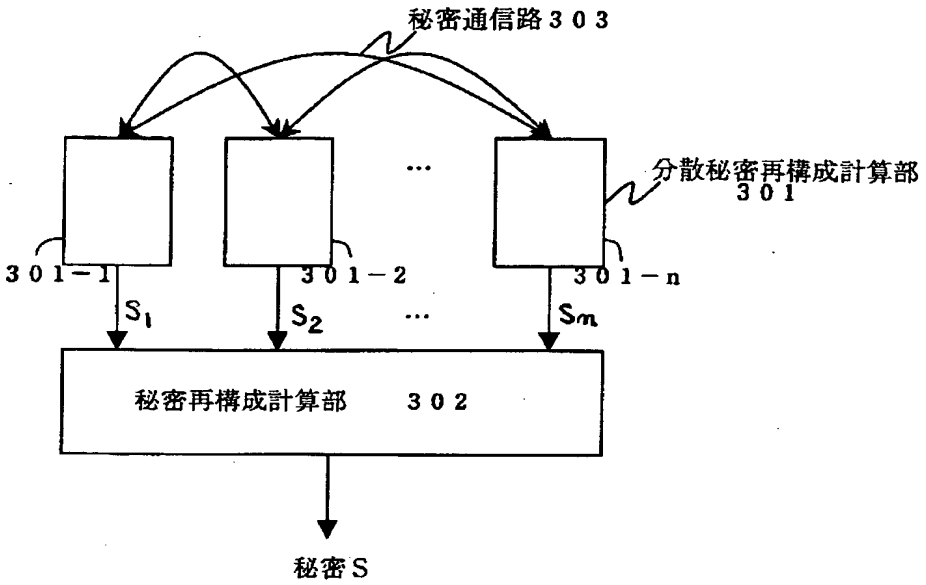
第１の実施形態における各メンバ及び秘密通信路

【図４】



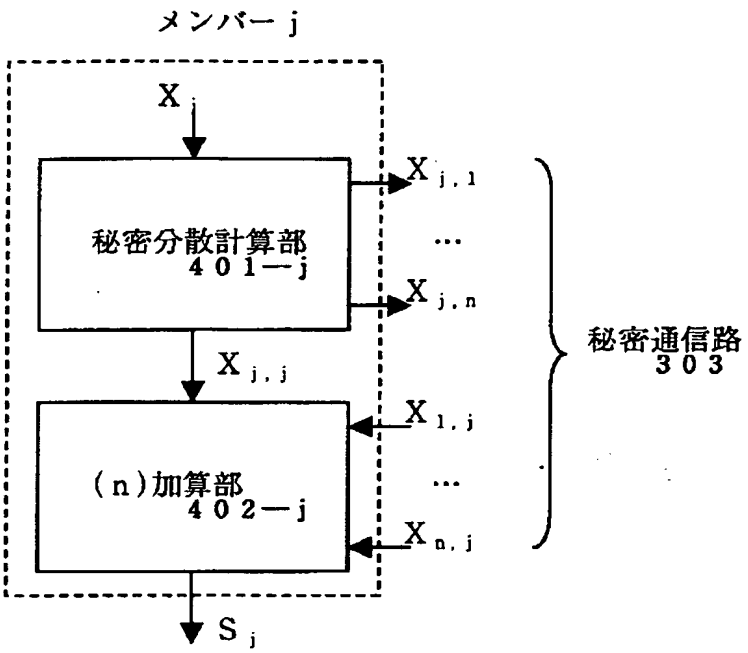
第１の実施形態の秘密再構成方法の概要

【図５】



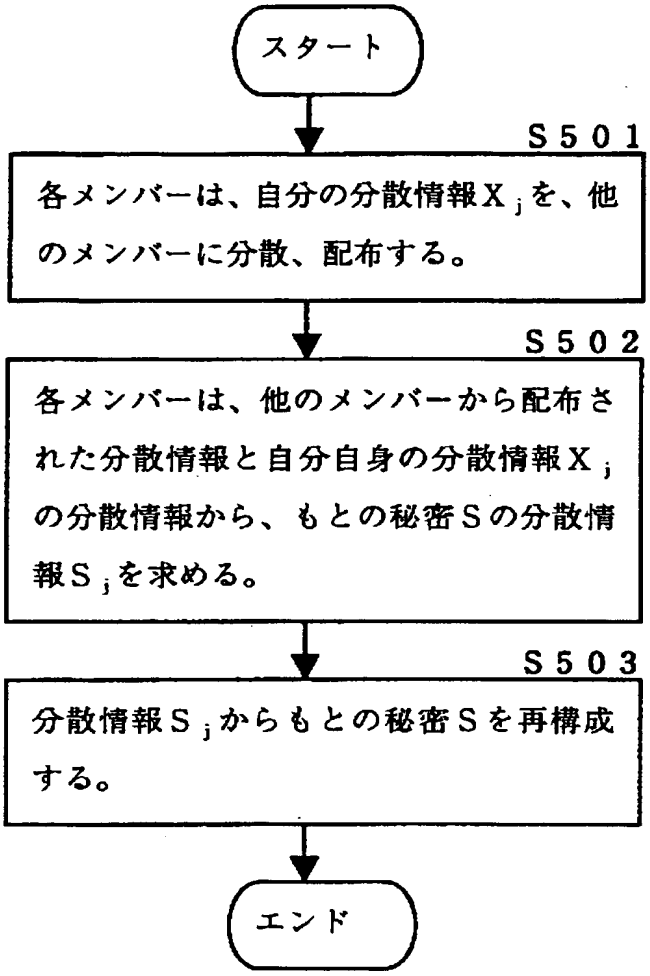
第１の実施形態の秘密再構成

【図６】



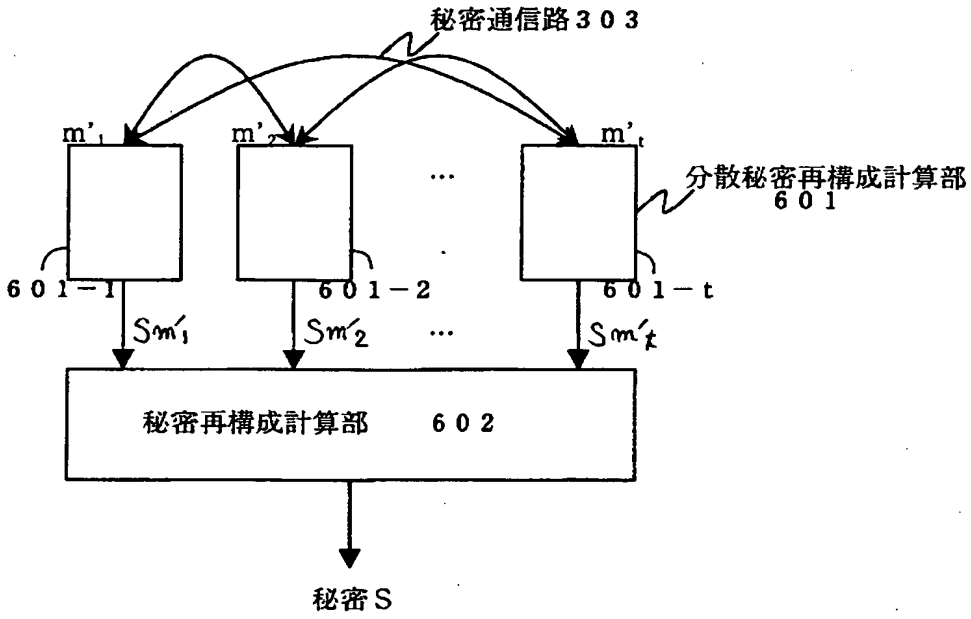
分散秘密再構成計算部３０１－ｊ

【図７】



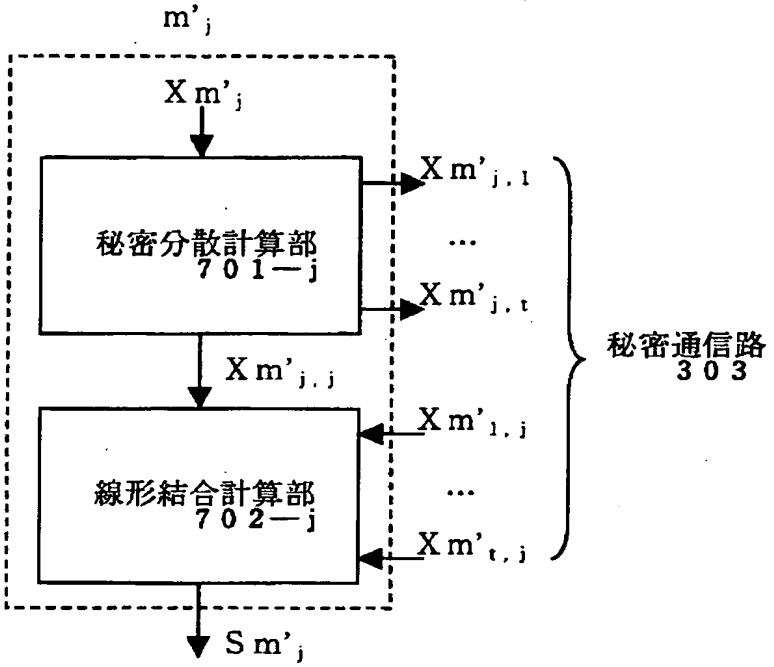
第１の実施形態の動作

【図８】



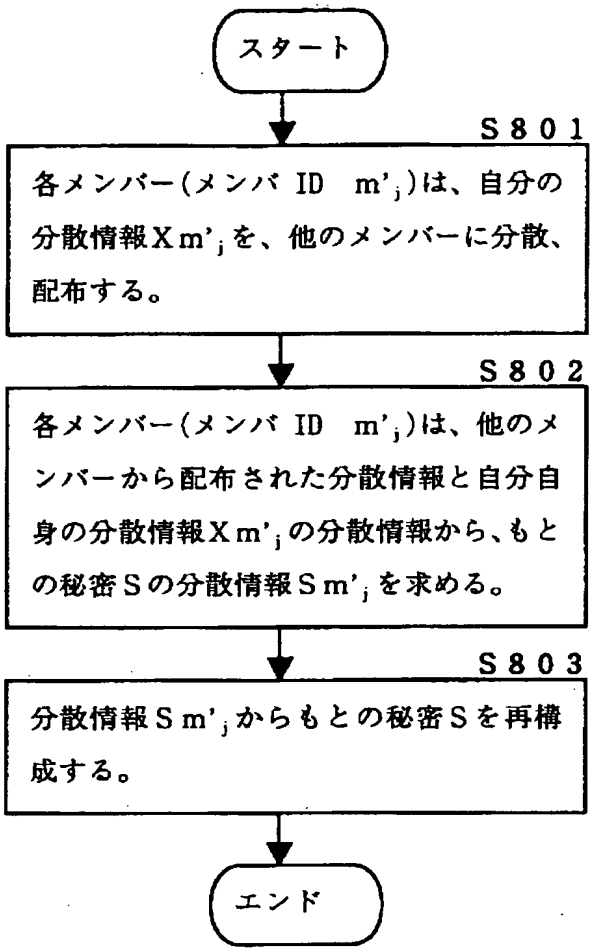
第２の実施形態の秘密再構成

【図９】



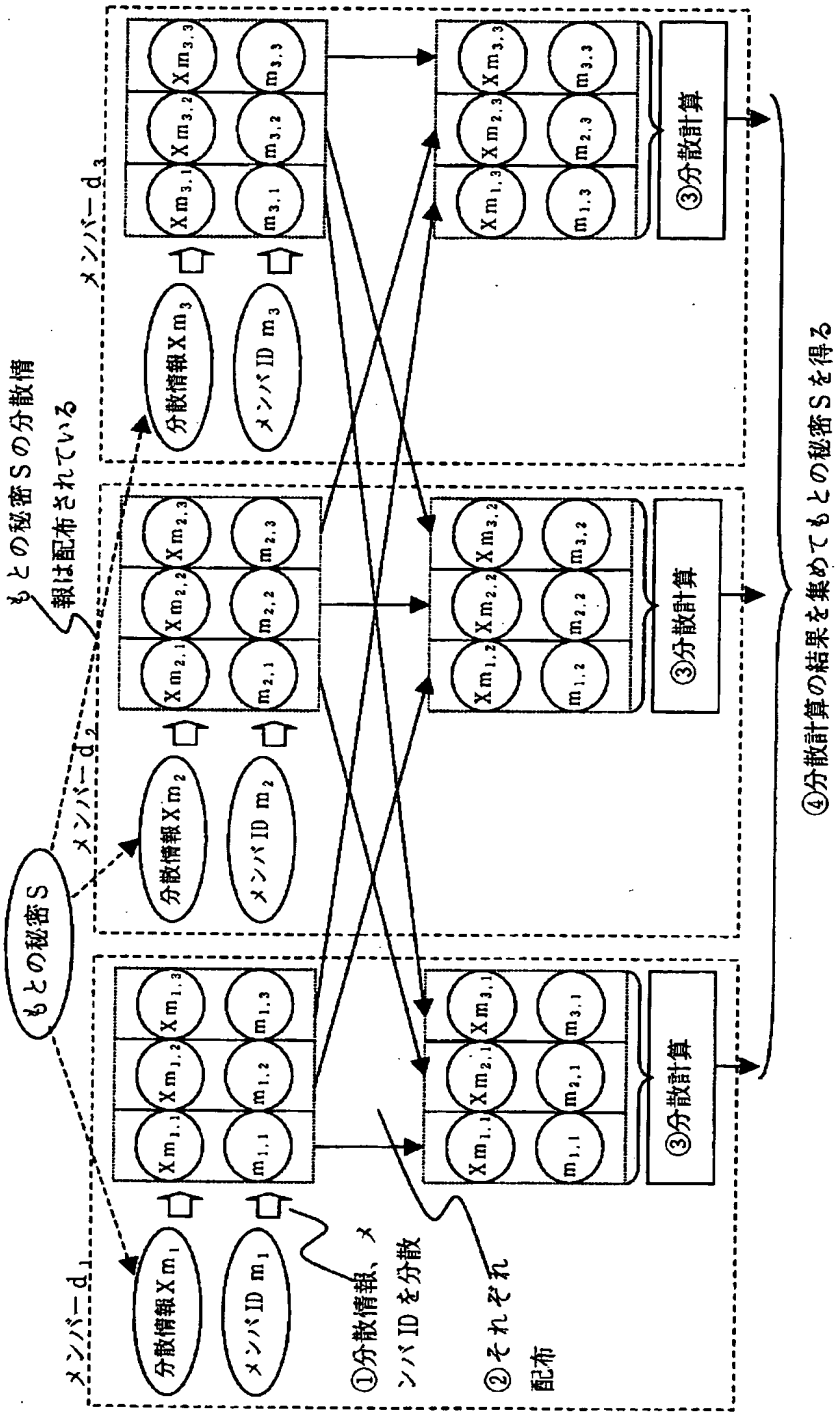
分散秘密再構成計算部６０１－ｊ

【図１０】



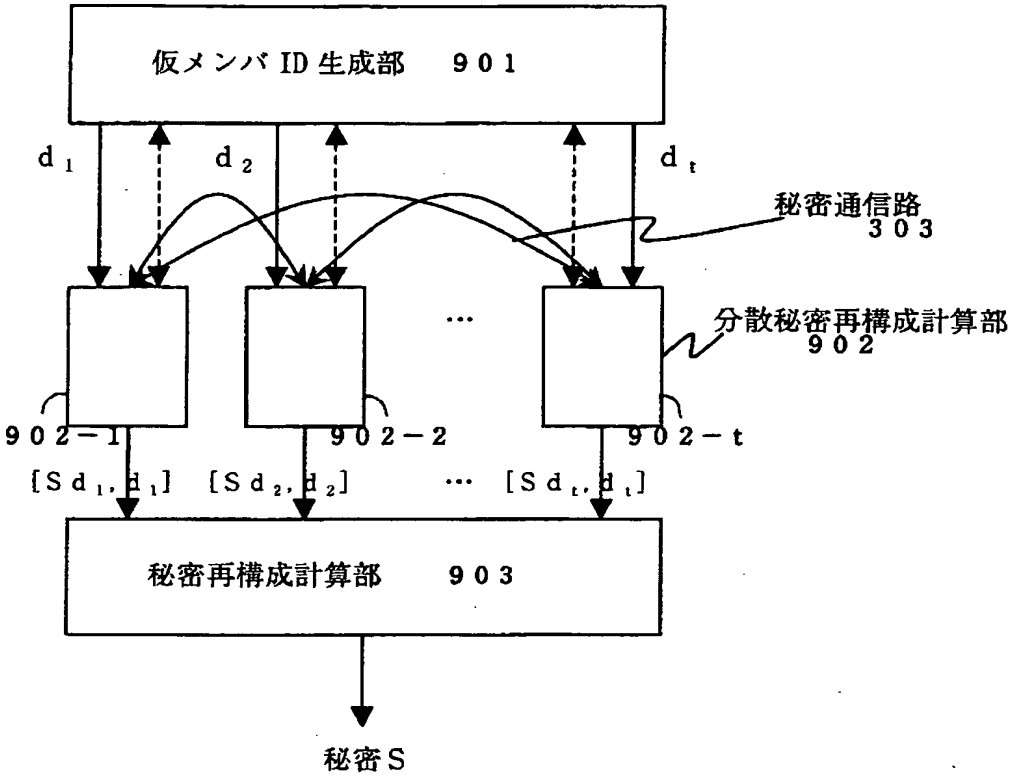
第２の実施形態の動作

【図１１】



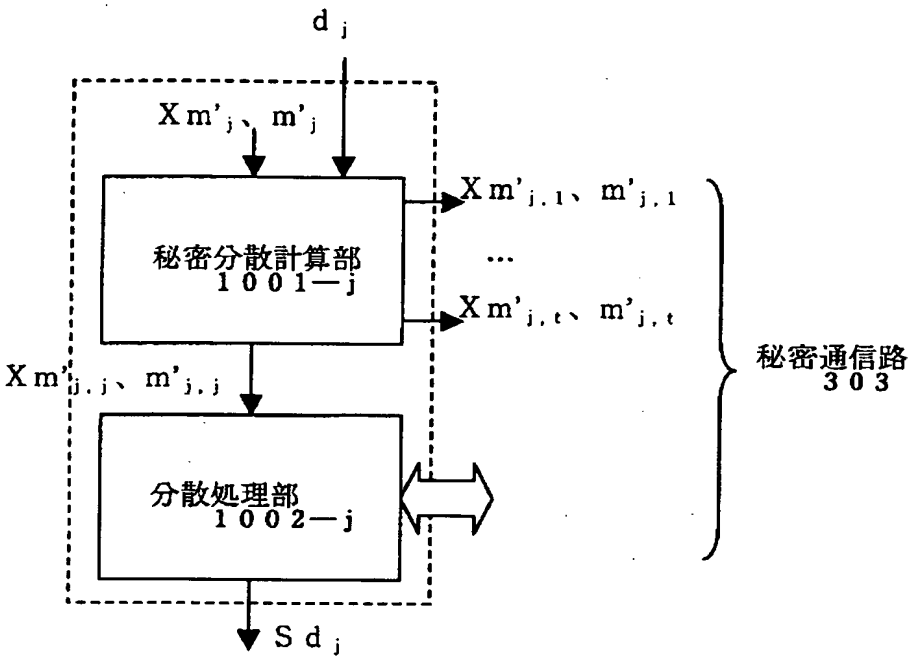
第３の実施形態の秘密再構成方法の概要

【図１２】



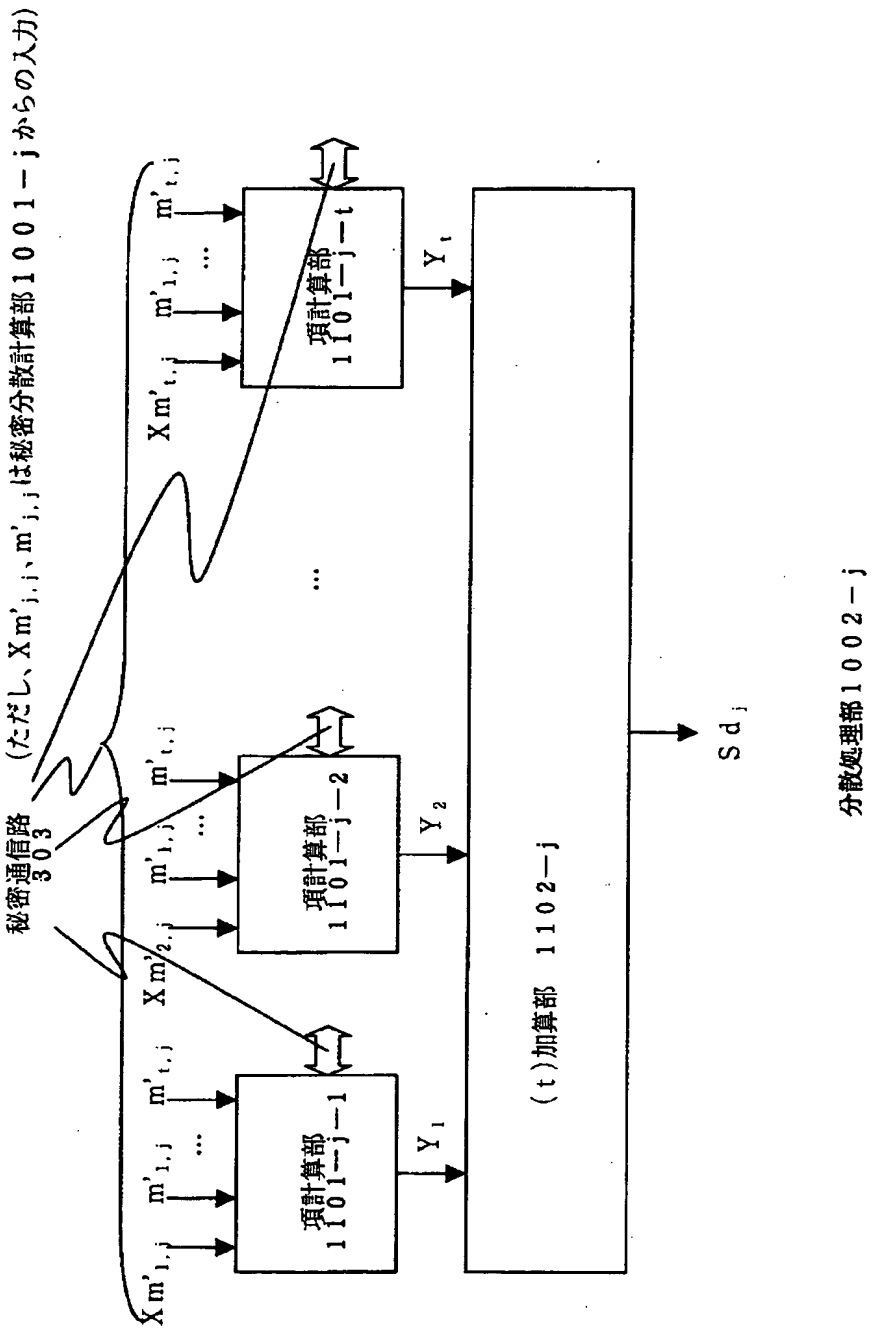
第３の実施形態の秘密再構成

【図１３】

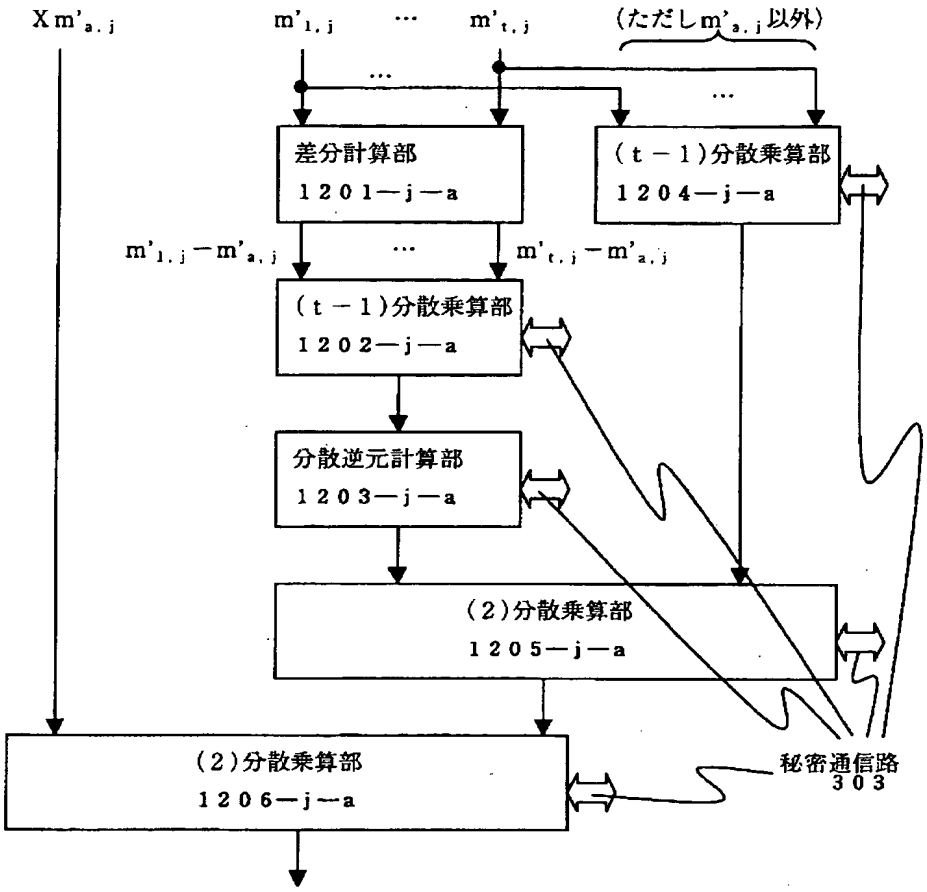


分散秘密再構成計算部９０２－j

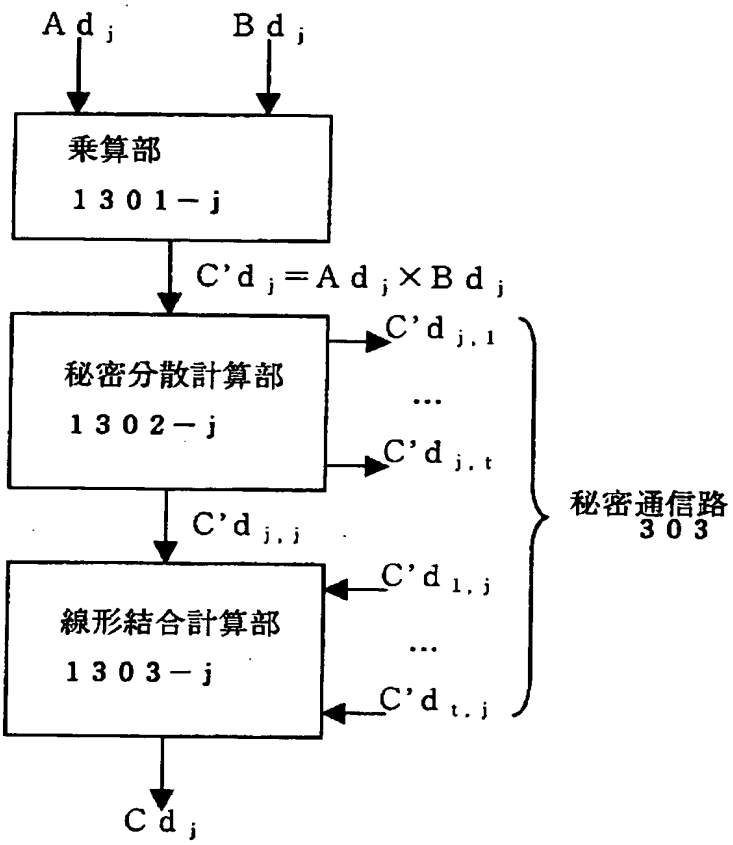
【図１４】


秘密通信路
３０３
(ただし、$Xm'_{j,j}$、$m'_{j,j}$は秘密分散計算部１００１－ｊからの入力)
$Xm'_{1,j}$
$Xm'_{2,j}$
$Xm'_{t,j}$
$m'_{1,j}$
$m'_{t,j}$
項計算部
１１０１－ｊ－１
項計算部
１１０１－ｊ－２
項計算部
１１０１－ｊ－ｔ
Y_1
Y_2
Y_t
(ｔ)加算部　１１０２－ｊ
Sd_j
分散処理部１００２－ｊ

【図１５】

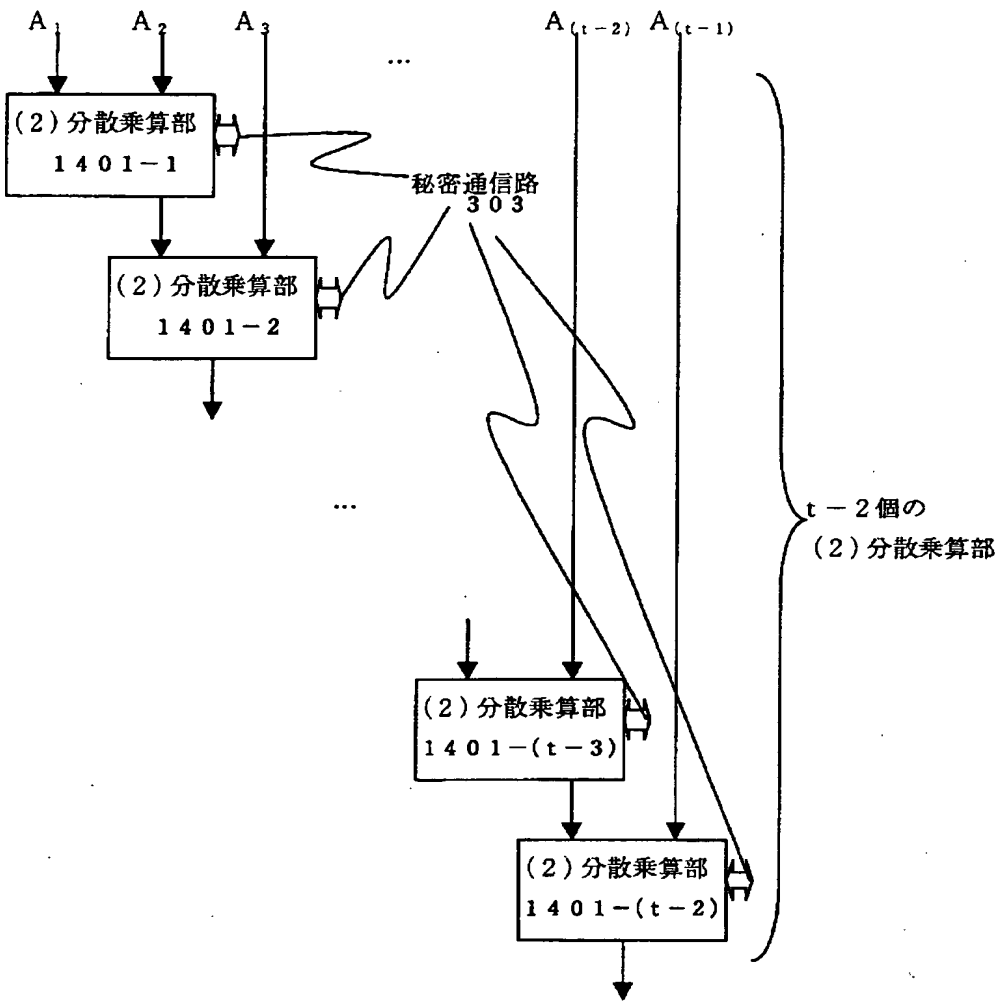

Xm'a,j
m'1,j … m't,j
(ただしm'a,j以外)
差分計算部
１２０１－ｊ－ａ
(ｔ－１)分散乗算部
１２０４－ｊ－ａ
m'1,j－m'a,j … m't,j－m'a,j
(ｔ－１)分散乗算部
１２０２－ｊ－ａ
分散逆元計算部
１２０３－ｊ－ａ
(２)分散乗算部
１２０５－ｊ－ａ
(２)分散乗算部
１２０６－ｊ－ａ
秘密通信路
３０３
項計算部１１０１－ｊ－ａ

【図１６】



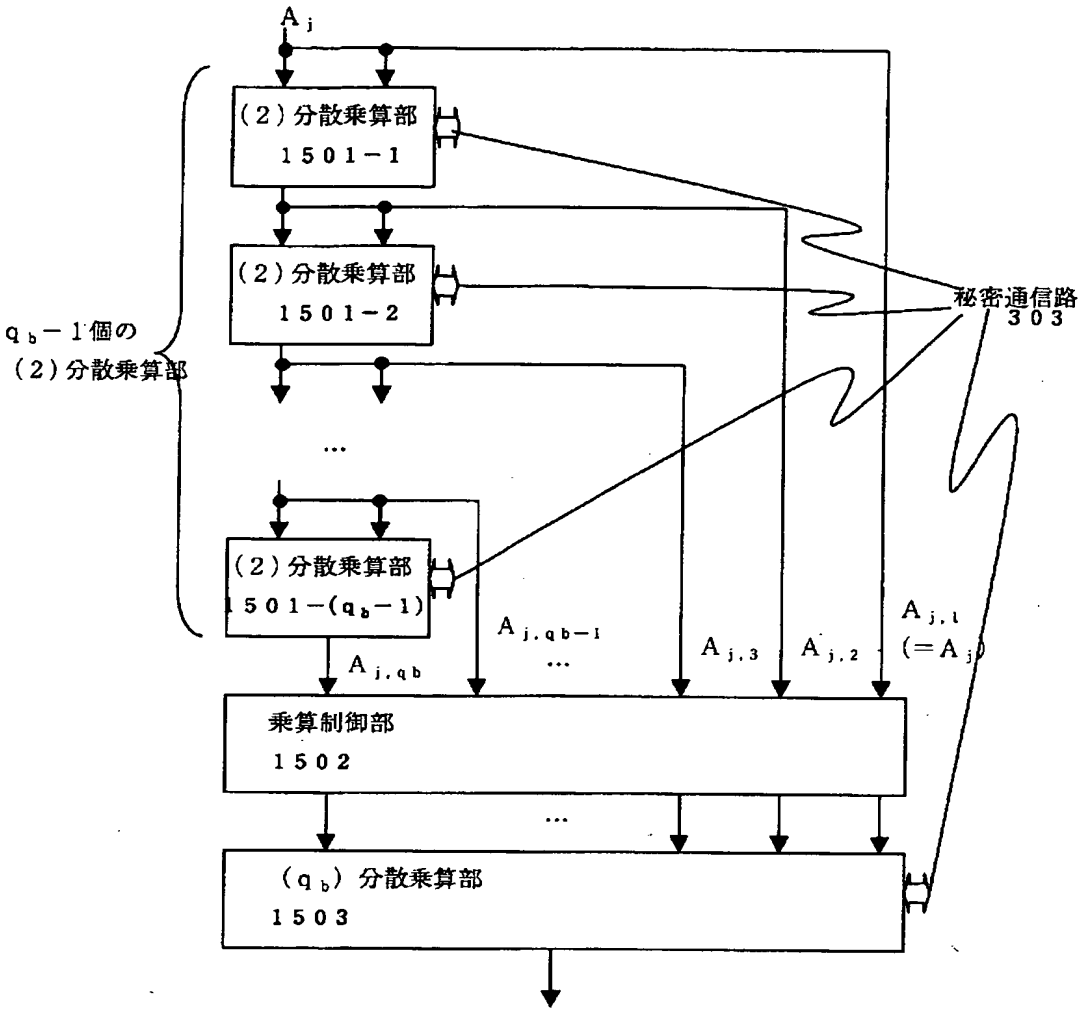
(2)分散乗算部１２０５－ｊ－ａ、１２０６－ｊ－ａ

【図１７】



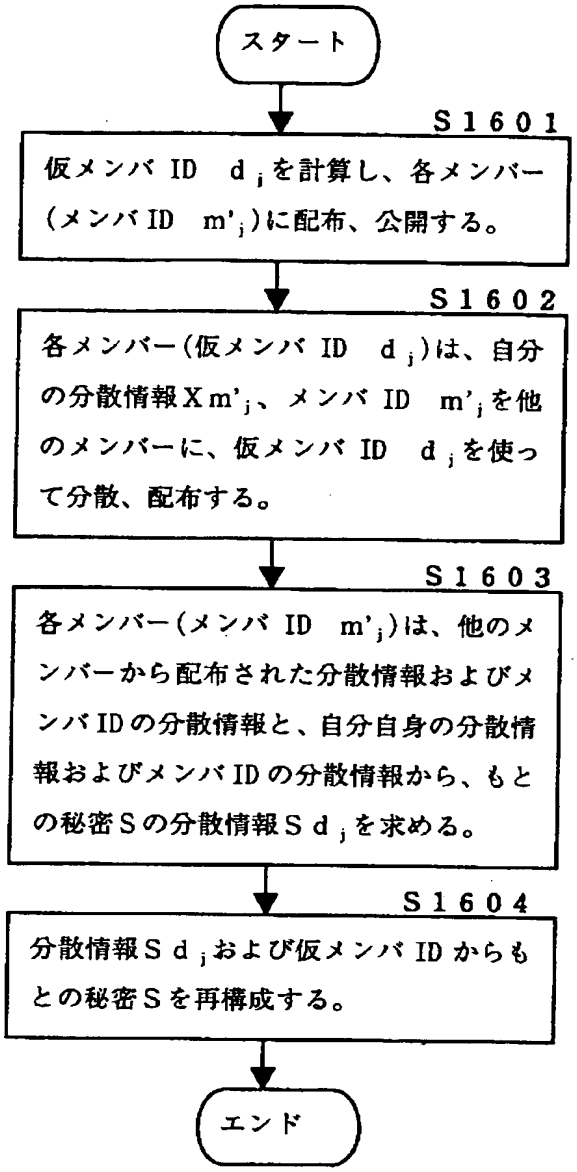
(t－1)分散乗算部１２０２－ｊ－ａ、１２０４－ｊ－ａ

【図１８】



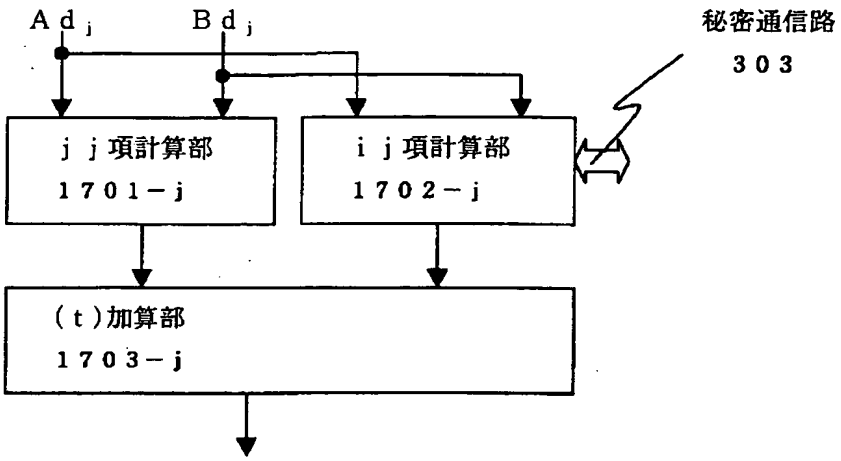
分散逆元計算部１２０３－ｊ－ａ

【図１９】



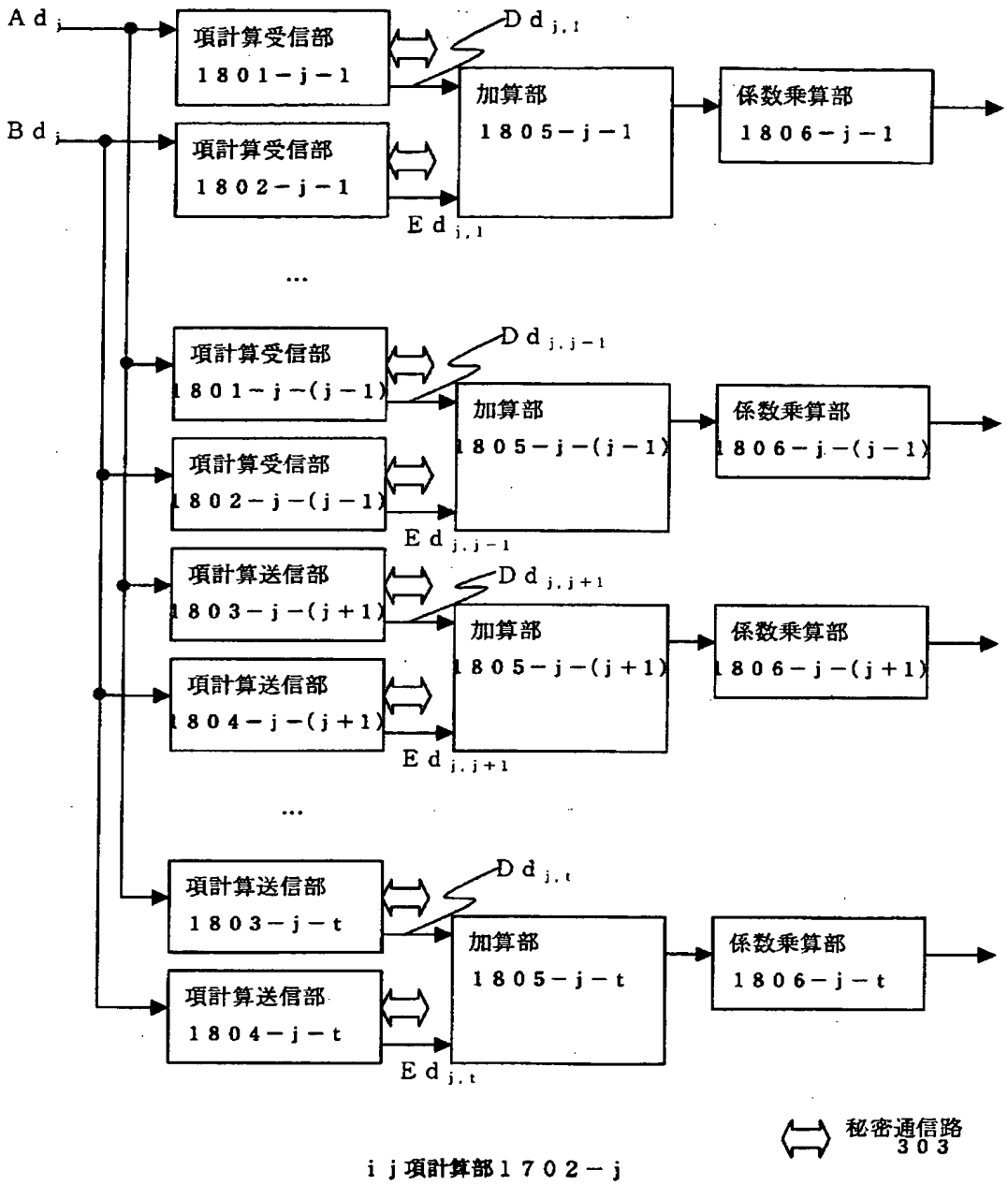
第３の実施形態の動作

【図２０】



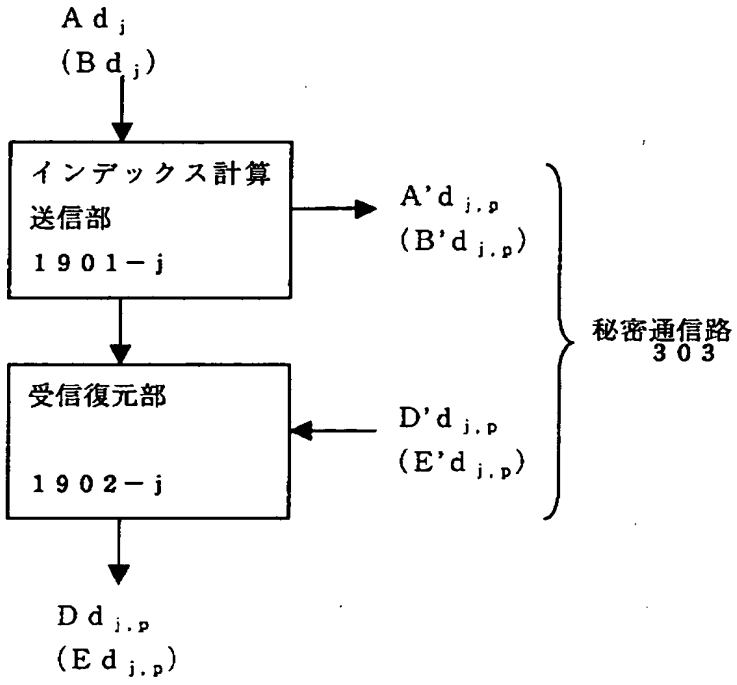
(2)分散乗算部１２０５－ｊ－ａ、１２０６－ｊ－ａ　（第４の実施形態）

【図２１】



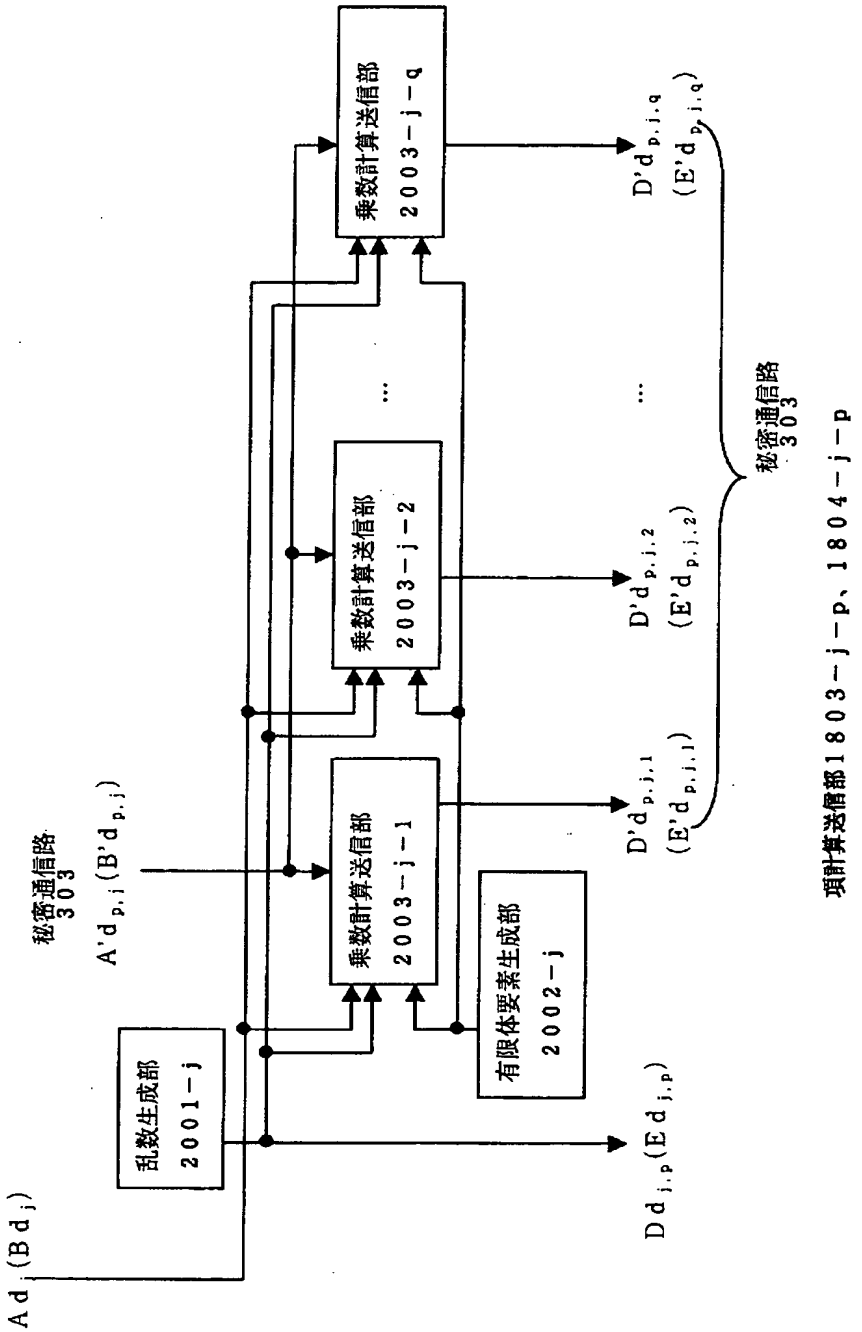
ｉｊ項計算部１７０２－ｊ

【図２２】

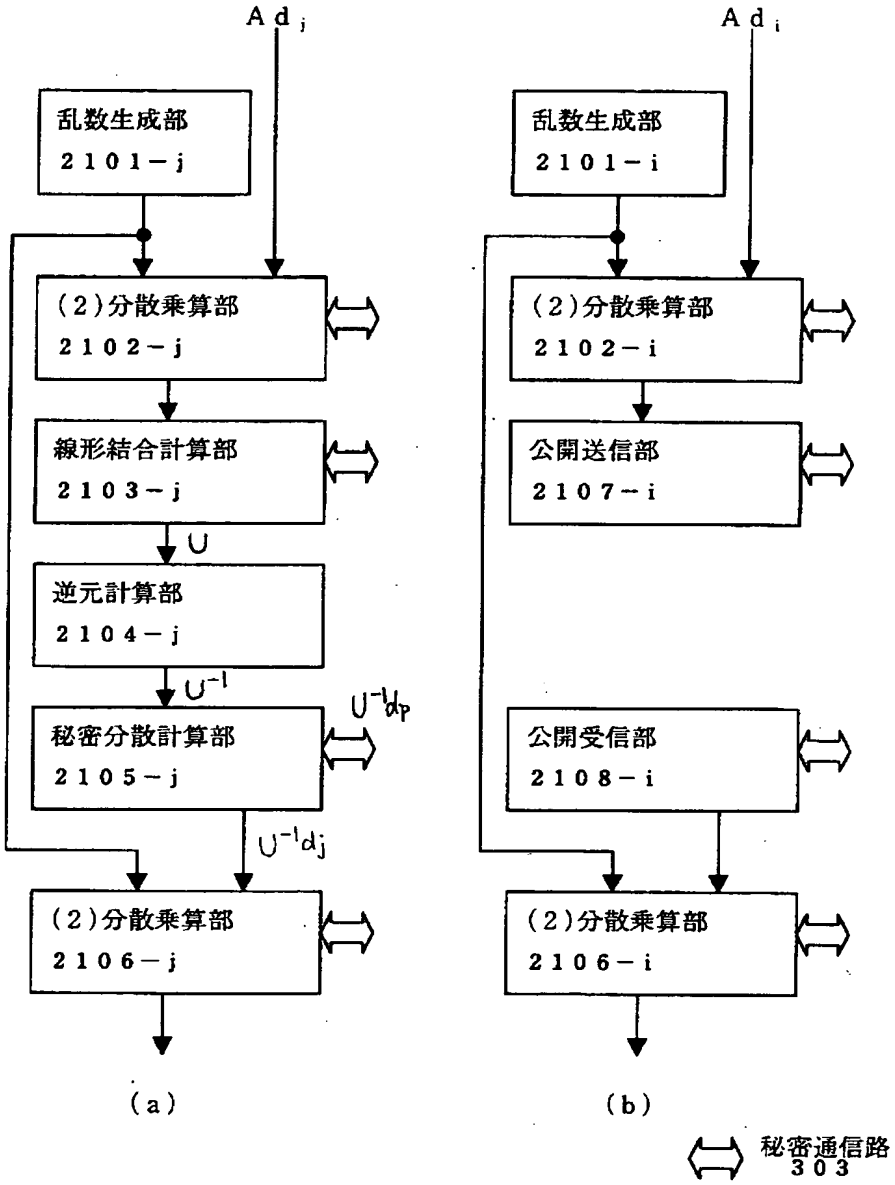


項計算受信部１８０１－ｊ－ｐ、１８０２－ｊ－ｐ

【図２３】

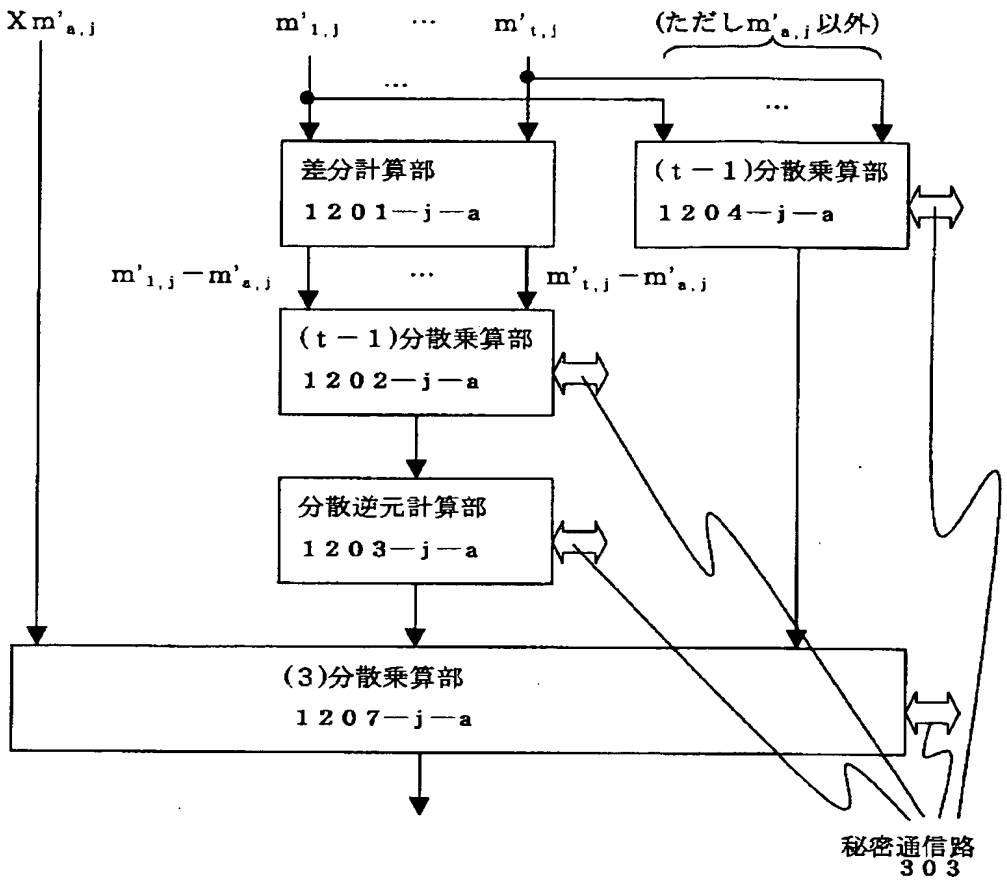

秘密通信路
３０３
乱数生成部
２００１－ｊ
有限体要素生成部
２００２－ｊ
乗数計算送信部
２００３－ｊ－１
乗数計算送信部
２００３－ｊ－２
乗数計算送信部
２００３－ｊ－ｑ
秘密通信路
３０３
項計算送信部１８０３－ｊ－ｐ、１８０４－ｊ－ｐ

【図２４】



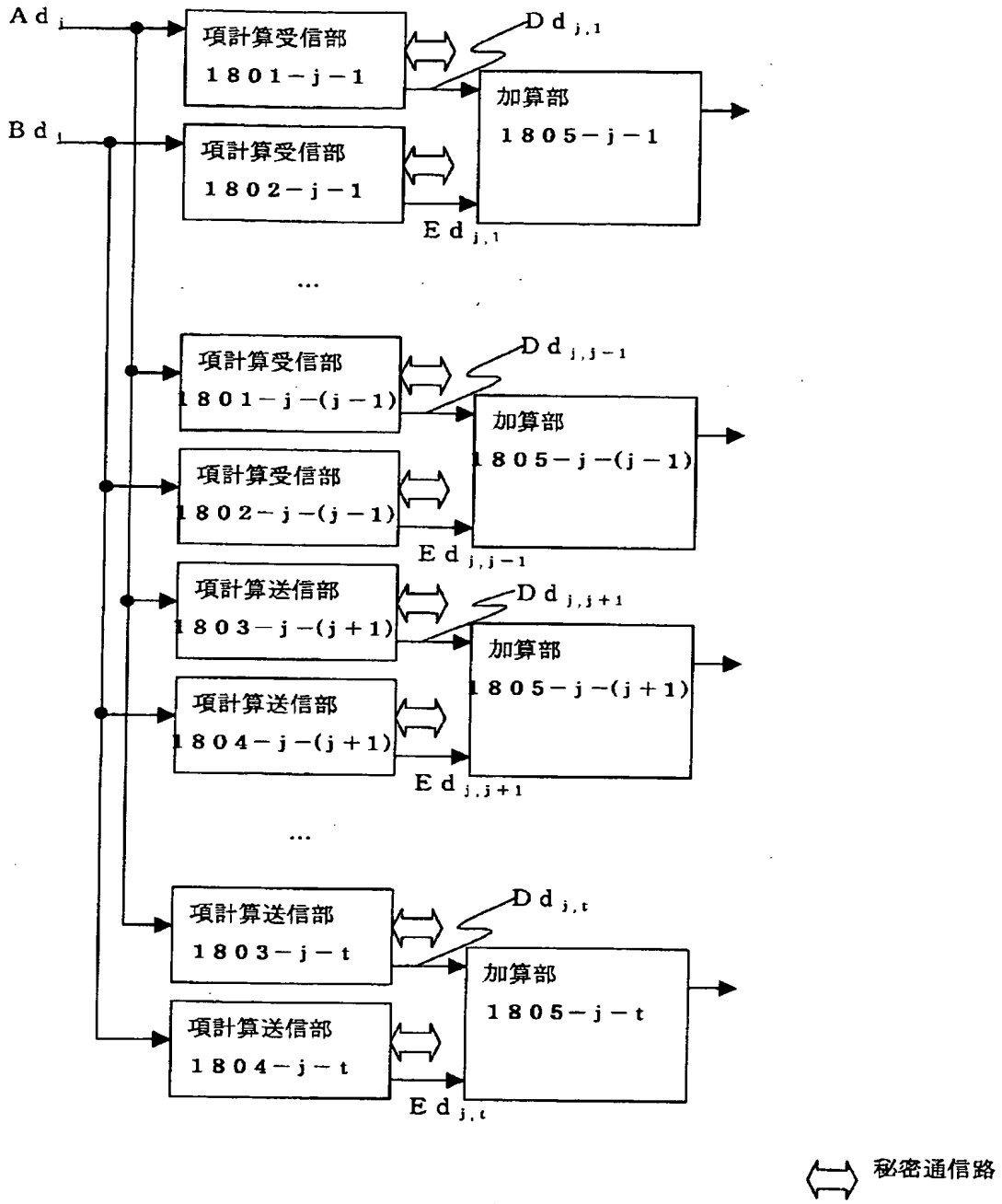
分散逆元計算部１２０３－ｊ－ａ　（第５の実施形態）

【図２５】



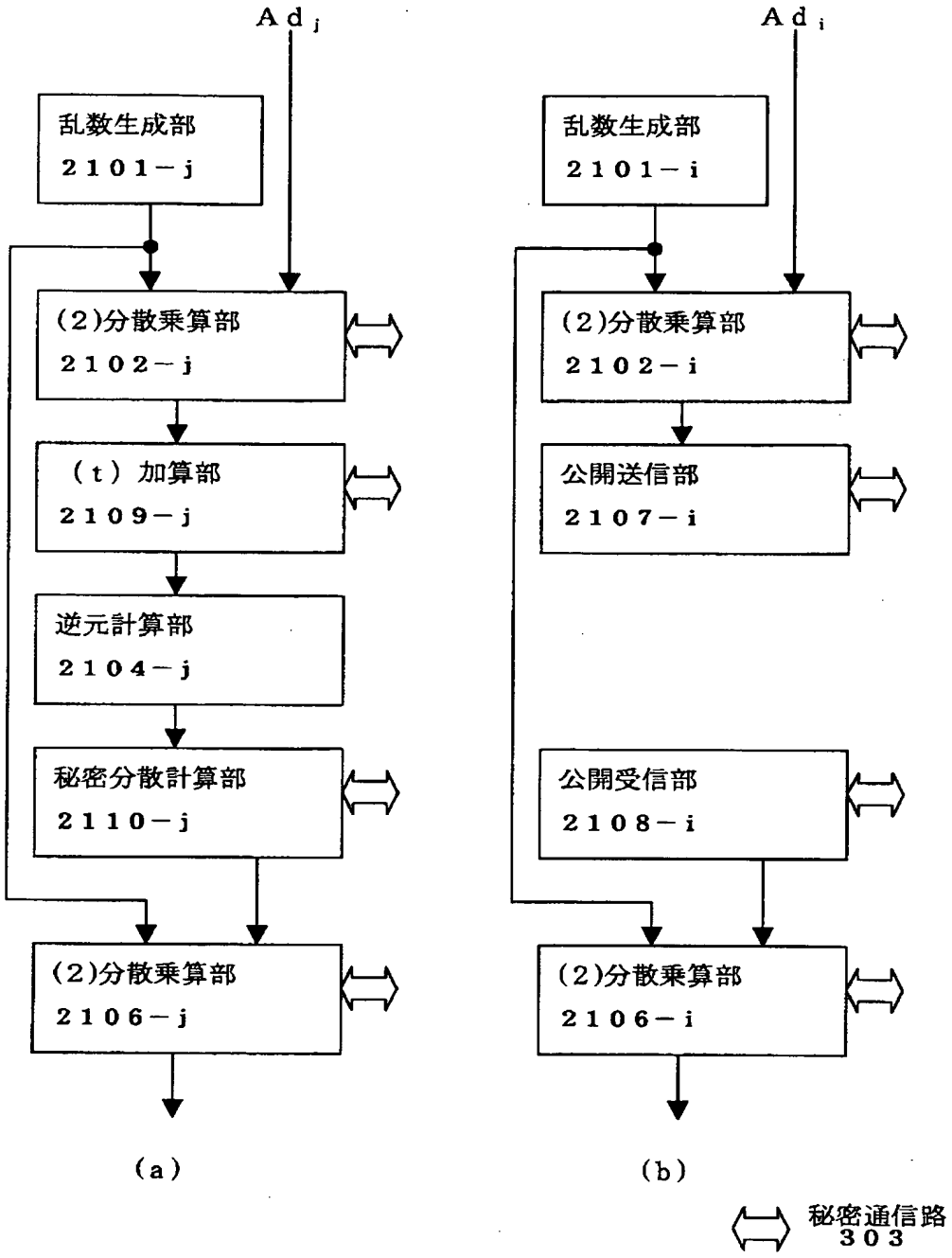
項計算部１１０１－ｊ－ａ(変形例)

【図２６】



ｉｊ項計算部１７０２－ｊ(変形例)

【図２７】



分散逆元計算部１２０３－ｊ－ａ（変形例）

【書類名】　　要約書

【要約】

【課題】　各メンバが保有する分散情報を公開せずに、もとの秘密情報の再構成を行う秘密再構成方法、分散秘密再構成装置、秘密再構成システムを提供する。

【解決手段】　秘密再構成方法は、ある秘密情報Ｓから第１の分散情報X_i（ｉ＝１，２，…，ｎ）を生成し各メンバに配布している場合に、ｔ（$2 \leqq t \leqq n$）人のメンバが集まって、もとの秘密情報Ｓを再構成する秘密再構成方法である。再構成に際しては、集まった各メンバにおいて、各自のメンバが持つ第１の分散情報X_iを秘密としたまま、秘密分散法を用いて第１の分散情報X_iを分散して第２の分散情報$X_{i,j}$（ｊ＝１，２，…，ｎ）として他の各メンバに対して配布し、他のメンバから第２の分散情報$X_{j,i}$を受け取ることにより、もとの秘密情報Ｓを再構成するための中間計算結果S_iを、分散計算により算出し、各メンバにおける中間計算結果S_iから、もとの秘密情報Ｓを再構成する。

【選択図】　　図５

出　願　人　履　歴　情　報

識別番号　　[０００００２９５]

１．変更年月日　　１９９０年　８月２２日
[変更理由]　　新規登録
住　所　　東京都港区虎ノ門１丁目７番１２号
氏　名　　沖電気工業株式会社